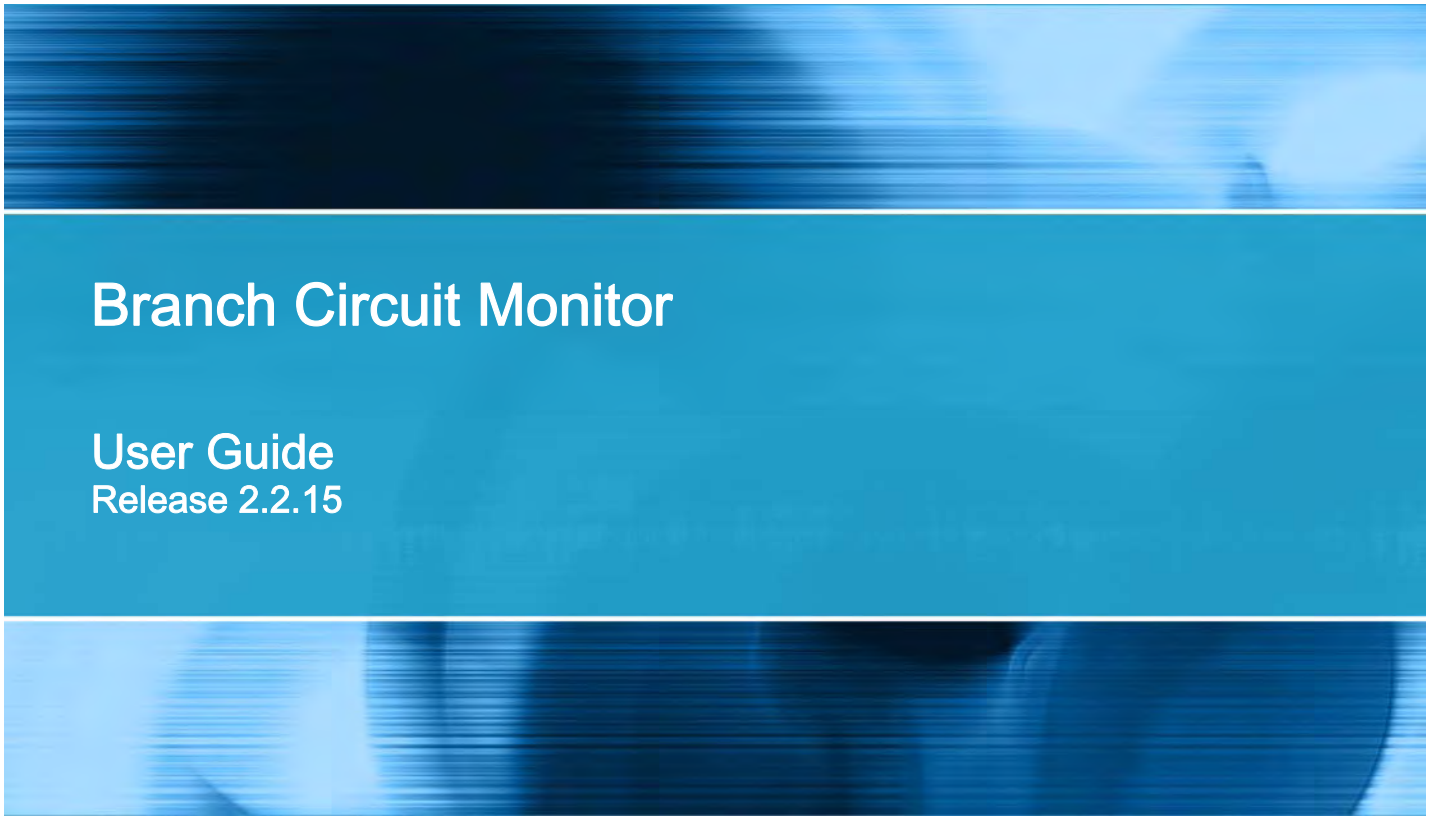


Branch Circuit Monitor

User Guide
Release 2.2.15

Copyright © 2012 Raritan, Inc.

BCM-0B-v2.2.15-E

January 2012

255-64-0002-00

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2012 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

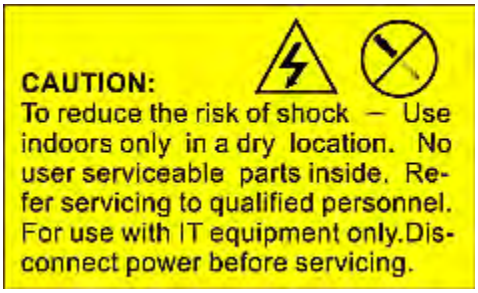
FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.


CAUTION:
To reduce the risk of shock — Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only.Disconnect power before servicing.

Safety Guidelines

WARNING! These instructions must be performed by a licensed electrician.

WARNING! Raritan products must not be serviced while energized. When power is present, do not open any panels or service the line cord. Always disconnect the far end of the line cord from power before servicing. Servicing the product while energized may result in electric shock, fire, personal injury and death.

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to a 3-phase AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a 3-phase AC power source that is current limited by a suitably rated circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! A current transformer (CT) must never be operated when it is not connected to the Branch Circuit Monitor. Operating a CT "open circuit" will cause permanent damage to the CT.

WARNING! Snap CTs only onto circuit conductors that are properly insulated per national and local electrical codes. Failure to snap CTs onto properly insulated conductors may result in electric shock, fire, personal injury and death.

WARNING! Do not rely on the power data displayed by this product to determine whether power is being supplied on a particular circuit/line. Disconnect the device from the branch circuit before performing repair, maintenance or service on the device. Failure to disconnect a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Do not use this product to measure and monitor the power source that powers critical patient care equipment, fire or smoke alarm systems. Use of this product in such applications may result in personal injury and death.

WARNING! Installation of this product and CTs must be performed by a licensed electrician, and the power system monitored by this product must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Installation by unlicensed electricians or failure to select a suitably rated power system may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Instructions

1. Installation of this product and current transformers (CTs) should only be performed by a licensed electrician.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. The Branch Circuit Monitor must be mounted inside the panel board it is monitoring. Do NOT mount it outside the panel because its flexible cord is not rated for a permanent electrical connection outside the panel.
4. Connect the line cord of this product only to a 3-phase AC power source that is current limited by a suitably rated branch circuit breaker in accordance with national and local electrical codes.
5. Examine the branch circuit that will supply electric power to this product. Make sure the branch circuit's power lines, neutral and protective earth ground terminals are wired correctly and are the correct voltage and phase. Make sure the branch circuit is protected by a suitably rated circuit breaker.
6. Before installing CTs, make sure there are no damages, cuts or wear on the insulation of CT leads.
7. Do NOT operate a CT when it is not connected to the Branch Circuit Monitor. Operating a CT “open circuit” causes permanent damage to the CT. Make sure the branch circuit breaker is turned OFF before snapping the CT onto a branch circuit conductor and do NOT turn the breaker on until the CT is properly connected to the Branch Circuit Monitor.
8. Make sure that the circuit conductors that CTs will monitor are properly insulated per national and local electrical codes, and the conductor's insulation is at least 0.4mm thick.

Contents

Safety Guidelines iii

Safety Instructions iv

Chapter 1 Introduction 1

Overview 1
Product Models 1
Product Features 2
Package Contents 3

Chapter 2 Installation and Configuration 4

Before You Begin 4
Unpacking the Product and Components 4
Checking the AC Electrical Panel 5
Printing the Circuit Monitoring Worksheet 5
Observing the Safety Guidelines and Instructions 5
Channel Convention 6
Setting Up a Power Monitoring System 7
Raritan Current Transformers (Optional) 8
Configuring the Branch Circuit Monitor 14
Connecting the Branch Circuit Monitor to a Computer 15
Installing the USB-to-Serial Driver 15
Connecting the Branch Circuit Monitor to Your Network 17
Initial Network Configuration 18
Mapping Channels with Branch Circuits 24
Connecting Environmental Sensors (Optional) 26
About Contact Closure Sensors 28
How to Connect Differential Air Pressure Sensors 31

Connecting a Logitech Webcam (Optional) 32

Chapter 3 Panel Components 33

Line Cord 33
Channels 34
- Mains Channels 34
- Branch Circuit Channels 35
- CT Terminals and Buttons 35

Connection Ports 35
LCD Display Panel 36
- LCD Display 37
- Control Buttons 38
- Operating the LCD Display 38

Reset Button 42

Chapter 4 Using the Web Interface 43

Supported Web Browsers 43
Logging in to the Web Interface 44
- Login 44
- Changing Your Password 45

Logout 46
Introduction to the Web Interface 47
- Menus 48
- Dominion PX Explorer Pane 48
- Setup Button 51
- Status Bar 51
- Add Page Icon 52
- Logout Button 53
- Data Pane 53
- More Information 53

Viewing the Dashboard 58
Device Management 58
- Displaying the Device Information 59
- Naming the Branch Circuit Monitor 60
- Modifying the Network Configuration 60
- Modifying the Network Service Settings 66
- Setting the Date and Time 69
- Specifying the Device Altitude 72
- Setting Data Logging 73
- Configuring the SMTP Settings 74
- Setting the EnergyWise Configuration 75
- Rebooting the Branch Circuit Monitor Device 76

Channel Management 76
- Configuring the Mains Channels 76
- Configuring the Branch Circuit Channels 77
- Naming the Mains Channels 79
- Naming Branch Circuit Channels 79

Monitoring the Mains Channels 80
Monitoring the Branch Circuit Channels 81
Setting Power Thresholds 83
Setting the Mains Thresholds 83
Setting the Branch Circuit Thresholds 84
Bulk Configuration for Branch Circuit Thresholds 85
What is Deassertion Hysteresis? 86
What is Assertion Timeout? 88
User Management 88
Creating a User Profile 88
Modifying a User Profile 91
Deleting a User Profile 92
Changing the User List View 92
Setting Up Roles 93
Creating a Role 93
Modifying a Role 94
Deleting a Role 95
Changing the Role List View 95
Access Security Control 95
Forcing HTTPS Encryption 96
Configuring the Firewall 96
Setting Up User Login Controls 101
Setting Up Role-Based Access Control Rules 104
Setting Up an SSL Certificate 107
Certificate Signing Request 108
Creating a Self-Signed Certificate 110
Installing Existing Key and Certificate Files 111
Downloading Key and Certificate Files 112
Setting Up LDAP Authentication 112
Gathering the LDAP Information 113
Adding the LDAP Server Settings 113
Sorting the LDAP Access Order 116
Testing the LDAP Server Connection 116
Editing the LDAP Server Settings 117
Deleting the LDAP Server Settings 117
Disabling the LDAP Authentication 117
Enabling LDAP and Local Authentication Services 118
Configuring Event Rules 118
Components of an Event Rule 119
Creating an Event Rule 119
Sample Event Rules 125
Modifying an Event Rule 126
Modifying an Action 127
Deleting an Event Rule or Action 128
A Note about Untriggered Rules 128
Managing Event Logging 128
Viewing the Local Event Log 129
Clearing Event Entries 129
Viewing Connected Users 130
Monitoring Server Accessibility 131
Adding IT Devices for Ping Monitoring 131
Editing Ping Monitoring Settings 132

Deleting Ping Monitoring Settings 132
Checking Server Monitoring States 132
Environmental Sensors 133
Identifying Environmental Sensors 134
Managing Environmental Sensors 135
Configuring Environmental Sensors 136
Viewing Sensor Data 139
Unmanaging Environmental Sensors 142
Copying Configurations with Bulk Configuration 143
Saving a Branch Circuit Monitor Configuration 144
Copying a Branch Circuit Monitor Configuration 145
Changing the Measurement Units 145
Viewing the Webcam Images or Videos 147
Network Diagnostics 147
Pinging a Host 148
Tracing the Network Route 148
Listing TCP Connections 148
Viewing the Communication Log 149
Downloading Diagnostic Information 150
Firmware Upgrade 150
Updating the Branch Circuit Monitor Firmware 151
Viewing Firmware Update History 152
Full Disaster Recovery 152
Accessing the Help 153
Retrieving Software Packages Information 153
Browsing through the Online Help 153

Chapter 5 Using SNMP 155

Enabling SNMP 155
Configuring Users for Encrypted SNMP v3 156
Configuring SNMP Traps 157
SNMP Gets and Sets 158
The Branch Circuit Monitor MIB 158
A Note about Enabling Thresholds 160

Chapter 6 Using the Command Line Interface 161

About the Interface 161
Logging in to CLI 161
With HyperTerminal 162
With SSH or Telnet 163
Different CLI Modes and Prompts 164
Closing a Serial Connection 164
Help Command 164
Showing Information 165
Network Configuration 165
Device Configuration 167
Branch Circuit Information 168

Mains Information 169
Environmental Sensor Information 170
Branch Circuit Threshold Information 171
Branch Circuit Pole Threshold Information 172
Mains Threshold Information 174
Mains Pole Threshold Information 175
Environmental Sensor Threshold Information 176
Security Settings 177
Existing User Profiles 177
Existing Roles 178
EnergyWise Settings 178
Reliability Data 178
Reliability Error Log 179
Command History 179
History Buffer Length 179
Examples 179
Configuring the Branch Circuit Monitor Device and Network 180
Entering the Configuration Mode 181
Device Configuration Commands 181
Networking Configuration Commands 184
Security Configuration Commands 207
Branch Circuit Channel Configuration Commands 227
Mains Channel Configuration Commands 228
Environmental Sensor Configuration Commands 228
Sensor Threshold Configuration Commands 233
User Configuration Commands 270
Role Configuration Commands 281
EnergyWise Configuration Commands 286
Setting the History Buffer Length 289
Multi-Command Syntax 289
Quitting the Configuration Mode 290
Unblocking a User 291
Resetting the Branch Circuit Monitor 291
Restarting the Device 291
Resetting to Factory Defaults 292
Network Troubleshooting 292
Entering the Diagnostic Mode 292
Diagnostic Commands 292
Quitting the Diagnostic Mode 295
Querying Available Parameters for a Command 296
Retrieving Previous Commands 296
Automatically Completing a Command 296
Logging out of CLI 297

Appendix A Specifications 298

Branch Circuit Monitor Specifications 298
CT Specifications 298
Power Measurement Accuracy 300
Mains Accuracy 300

Branch Circuit Accuracy 301
Maximum Ambient Operating Temperature 301
Serial RS-232 Port Pinouts 301
Sensor RJ-12 Port Pinouts 302

Appendix B Circuit Monitoring Worksheet 303

Appendix C Resetting to Factory Defaults 304

Using the Reset Button 304
Using the CLI Command 305

Appendix D LDAP Configuration Illustration 306

Step A. Determine User Accounts and Groups 306
Step B. Configure User Groups on the AD Server 307
Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device 308
Step D. Configure Roles on the Branch Circuit Monitor 311

Appendix E Additional Branch Circuit Monitor Information 315

Altitude Correction Factors 315
RF Code Energy Monitoring Solution 316

Index 317

Chapter 1 Introduction

This chapter briefly introduces the Raritan Branch Circuit Monitor (BCM) and current transformers (CTs), which provide a centralized power monitoring solution at the circuit level.

In This Chapter

Overview....1
Product Models....1
Product Features....2
Package Contents....3

Overview

The Branch Circuit Monitor (BCM) is a product that is designed to measure and display the power and energy consumption of multiple branch circuits. Currently the Branch Circuit Monitor only applies to a 3-phase wye-connected electrical panel that is rated up to 200A and contains at least one 3-phase branch circuit breaker rated at 20A (North America) or 16A (Europe).

Use of this product helps you do the following at the CIRCUIT level:

- Monitor the power and energy consumption
- Analyze and optimize the power efficiency
- Avoid potential overload risks

To establish such a centralized power monitoring system, the items below are required:

- A Branch Circuit Monitor: You can remotely monitor the power and energy consumption of each conductor in the electrical panel through the Branch Circuit Monitor.
- Raritan CTs: A CT can detect the current of the conductor where it is snapped, and transmit the data to the Branch Circuit Monitor where it is connected. There are two types of CTs: mains CTs for monitoring mains circuits and branch circuit CTs for monitoring branch circuits.

Product Models

The Branch Circuit Monitor comes in several models that are built to stock and can be obtained almost immediately. Raritan also offers custom models that are built to order and can only be obtained on request.

Product Features

The Branch Circuit Monitor features include:

- The ability to monitor the following at the mains level:
  - RMS current per line (A)
  - RMS voltage per line pair (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage
- The ability to monitor the following at the branch circuit level:
  - RMS current (A)
  - RMS voltage (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage (for a 3-phase branch circuit only)

Note: The Branch Circuit Monitor only supports measuring and monitoring single-phase and 3-phase branch circuits.

- The ability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- Configurable alarm thresholds and hysteresis
- Configurable assertion timeout for thresholds
- Support for SNMP v1, v2, and v3
- The ability to send traps using the SNMP protocol
- The ability to retrieve branch circuit specific data using SNMP, including current, voltage, and power
- The ability to store a data log of all sensor measurements and retrieve it via SNMP

Note: Raritan's Power IQ or other external systems can retrieve the stored data (samples) from the Branch Circuit Monitor.

- The ability to configure and set values through SNMP, including power threshold levels
- The ability to save one Branch Circuit Monitor device's configuration settings and then deploy those settings to other Branch Circuit Monitor devices
- Support for both of IPv4 and IPv6 networking
- Support for Baytech BSNMP
- Support for Cisco EnergyWise
- Support for RF Code energy monitoring system
- The ability to diagnose the network, such as pinging a host or listing TCP connections
- The ability to monitor sever accessibility
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade
- The ability to display temperatures in Celsius or Fahrenheit, height in meters or feet, and pressure in Pascal or psi according to user credentials
- The ability to visually monitor the environment through a connected Logitech® QuickCam® Pro 9000 Webcam

Package Contents

The following describes the equipment shipped with a Branch Circuit Monitor device. If anything is missing or damaged, contact the local dealer or Raritan Technical Support for help.

- The Branch Circuit Monitor
- Ring terminals
- Split-core mains current transformers (Optional)
- Split-core branch circuit current transformers (Optional)
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable ties

Chapter 2 Installation and Configuration

This chapter explains how to install a Branch Circuit Monitor device and configure it for network connectivity.

In This Chapter

Before You Begin 4
Channel Convention 6
Setting Up a Power Monitoring System.....7
Configuring the Branch Circuit Monitor 14
Mapping Channels with Branch Circuits.....24
Connecting Environmental Sensors (Optional) 26
Connecting a Logitech Webcam (Optional).....32

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Check the AC electrical panel
- Print the Circuit Monitoring Worksheet
- Review the safety guidelines and instructions

Unpacking the Product and Components

1. Remove the Branch Circuit Monitor device and other equipment from the box in which they were shipped. See ***Package Contents*** (on page 3) for a complete list of the contents of the box.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Raritan's Technical Support Department for assistance.

Checking the AC Electrical Panel

A Branch Circuit Monitor is used to measure and monitor multiple circuits of an AC electrical panel. Before installing this product, verify that the electrical panel satisfies the following requirements:

- A three-phase wye-connected AC power system.
- The current and voltage ratings meet the ratings specified on the Branch Circuit Monitor's nameplate or label.
- Contains at least one 3-phase branch circuit breaker rated at 20A or 16A, conforming to national and local codes, such as UL508A Sec.17.5 in North America or EN/IEC 60934 and VDE 0642 in Europe. The Branch Circuit Monitor must be connected to a 3-phase branch circuit for electricity reception.
- Free of extreme temperatures and humidity. See ***Maximum Ambient Operating Temperature*** (on page 301) in the Branch Circuit Monitor User Guide.

For example, an electrical panel must meet the following for a BCM-2400 model:

Power system	Three-phase wye-connected
Rated current	Max. 200A
Rated voltage	190 to 415VAC
Circuit breaker	Contains at least one 3-phase branch circuit breaker rated at 20A or 16A

Printing the Circuit Monitoring Worksheet

A Circuit Monitoring Worksheet is provided in this guide. See ***Circuit Monitoring Worksheet*** (on page 303). Use this worksheet to record the panel number of the branch circuits monitored by the Branch Circuit Monitor, and usage of each branch circuit.

As you add, remove or swap CTs and/or channels, keep the worksheet up-to-date.

Observing the Safety Guidelines and Instructions

1. Review the ***Safety Guidelines*** (on page iii) listed in the beginning of this user guide.
2. Review the ***Safety Instructions*** (on page iv) listed in the beginning of this user guide.

Channel Convention

Before installing the Branch Circuit Monitor, you should know how a "channel" is defined on the Branch Circuit Monitor.

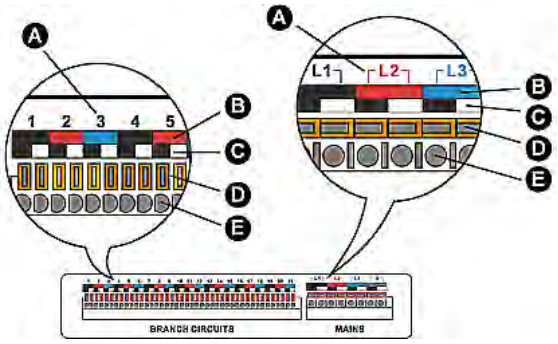
A channel on the Branch Circuit Monitor is used to monitor a circuit, which may be phase A, B or C. There are two types of channel groups: MAINS and BRANCH CIRCUITS. MAINS channels are for monitoring the main circuits, and BRANCH CIRCUITS channels are for branch circuits. The maximum current ratings supported by different channel groups are different. See the nameplate or label affixed to your Branch Circuit Monitor for appropriate ratings supported by each channel group.

Important: Mains and branch circuits that are monitored by a Branch Circuit Monitor must belong to the same electrical panel.

A channel is identified with a channel number and a channel color. A "black" channel is to monitor phase A, a "red" channel to phase B and a "blue" channel to phase C.

A channel comprises two CT terminals for connecting to one CT. Because a Raritan CT has two leads, which are marked with either the black or white color, a CT terminal on the Branch Circuit Monitor is also marked with either color to identify which CT lead to plug.

The following diagram illustrates the channels on the BCM-2400 model.



Item	Description
A	Channel numbers
B	Channel colors for identifying the circuit to monitor: black for phase A, red for phase B and blue for phase C
C	Terminal colors for identifying which CT lead to connect: black or white
D	Terminal buttons for controlling the springs inside the corresponding CT terminals

Item	Description
E	CT terminals

Setting Up a Power Monitoring System

Both the Branch Circuit Monitor and CTs are required for establishing a power monitoring system on an electrical panel.

The Branch Circuit Monitor contains a flexible cord containing the five wires for a 5-wire (3P+N+PE) AC connection. Before setting up such a system, make sure the electrical panel has a 3-phase branch circuit to power the Branch Circuit Monitor.

To set up a power monitoring system:

1. Mount the Branch Circuit Monitor INSIDE the electrical panel that it will monitor because its flexible cord is not rated for a permanent electrical connection outside the panel. The Branch Circuit Monitor can be attracted to a metal surface due to its magnetic characteristic.
2. The Branch Circuit Monitor requires 3-phase AC power. Connect the Branch Circuit Monitor to one of the panel's 3-phase branch circuits by wiring the 5-wire flexible cord as shown below:
   a. Connect the L1 wire to a phase A connection point in the panel.
   b. Connect the L2 wire to a phase B connection point in the panel.
   c. Connect the L3 wire to a phase C connection point in the panel.
   d. Connect the N wire to the panel's neutral bus.
   e. Connect the GND wire to the panel's ground bus.
3. Snap mains CTs onto the mains circuit conductors of the panel, and then connect these CTs to the MAINS channels on the Branch Circuit Monitor. For details, see ***Connecting Mains CTs*** (on page 9).
   a. Connect the phase A CT to L1 on the Branch Circuit Monitor.
   b. Connect the phase B CT to L2 on the Branch Circuit Monitor.
   c. Connect the phase C CT to L3 on the Branch Circuit Monitor.

   Important: Do NOT plug any CT leads into the channel labeled N on the Branch Circuit Monitor because the Branch Circuit Monitor does not support measuring the neutral conductor.
4. Switch OFF the 1-pole or 3-pole circuit breaker(s) where the branch circuit CTs will monitor. **This step is required because operating a branch circuit CT while it is not connected to the Branch Circuit Monitor results in damage to the CT.**

   Note: The Branch Circuit Monitor does not support measuring 2-pole branch circuit breakers so do not use the CT with a 2-pole breaker.

5. Snap branch circuit CTs onto the panel's branch circuit conductors and connect them to the BRANCH CIRCUITS channels on the Branch Circuit Monitor. For details, see ***Connecting Branch Circuit CTs*** (on page 12).
   - Connect a phase A CT to a "black" channel on the Branch Circuit Monitor, such as channel #1, #4, #7, #10, and so on.
   - Connect a phase B CT to a "red" channel on the Branch Circuit Monitor, such as channel #2, #5, #8, #11 and so on.
   - Connect a phase C CT to a "blue" channel on the Branch Circuit Monitor, such as channel #3, #6, #9, #12 and so on.
   - For a 3-phase branch circuit connection, make sure all three CTs are connected to a group of three channels comprising black, red and blue channels in sequence. For example, connect the three CTs to channels #1 to #3, or #4 to #6, or #7 to #9, and so on.
   - Record the panel numbers of the branch circuits and the channel numbers of CTs. This information is required for mapping the branch circuits with the Branch Circuit Monitor's channels. You can use the ***Circuit Monitoring Worksheet*** (on page 303) provided in the Branch Circuit Monitor User Guide to note down this information.
6. Use cable ties provided by Raritan to secure CT leads in place, and make sure the CT leads do not touch any wire terminals on the electrical panel.
7. Verify that all CTs have been properly connected to the Branch Circuit Monitor.
8. Switch ON the branch circuit breakers where CTs are installed.

Raritan Current Transformers (Optional)

A current transformer (CT) can detect the current of the circuit conductor that passes through it and transmit the data to the Branch Circuit Monitor where it is connected.

Raritan provides two types of CTs: mains CTs and branch circuit CTs. Mains CTs are for main circuits rated up to 200A, and branch circuit CTs for branch circuits rated up to 30A. Both types are split-core CTs so they can be snapped onto a circuit conductor without disconnecting the conductor from the wire terminal of the electrical panel.

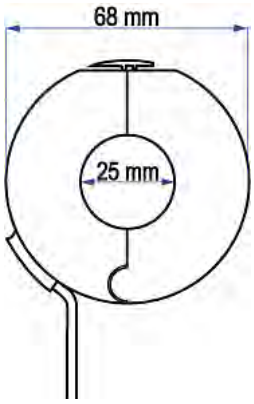
Each CT has a black lead and a white lead, which are inserted into the CT terminals on the Branch Circuit Monitor.

Important: The CT lead's color must be identical to the color of the CT terminal where it is plugged. Otherwise, the CT signals are reversed and the Branch Circuit Monitor incorrectly measures the current values.

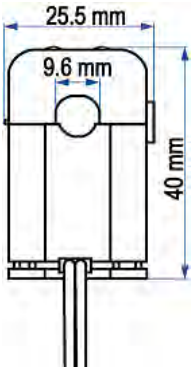
CT Dimensions

Sizes of mains CTs and branch circuit CTs are different.

Mains CT

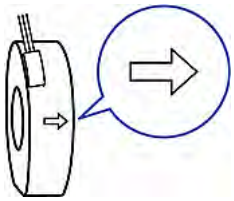


Branch circuit CT



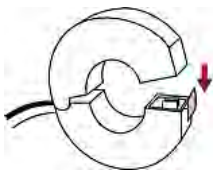
Connecting Mains CTs

When snapping the CT onto a circuit conductor, make sure the CT's arrow mark points towards the load. For mains CTs, the arrow mark is on one side of the CT. Note that this arrow is NOT the one shown on the CT's release tab.



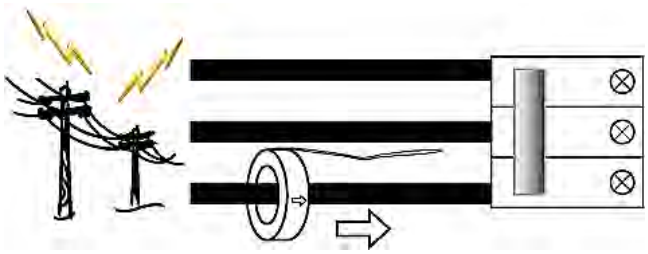
To connect mains CTs:

1. Verify the mains to monitor meets the maximum current rating specified for the MAINS channels on the Branch Circuit Monitor's nameplate or label.
2. Open the CT by unlocking its release tab. An arrow marked on the release tab indicates the correct direction to open the mains CT.



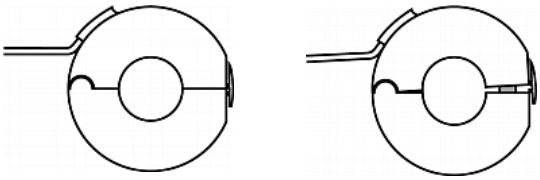
3. Slip the CT over the mains phase A conductor and snap it.

- Make sure the direction of the arrow on one side of the CT is the same as the following illustration.



- Make sure the CT's release tab is locked properly.

Proper **Improper**

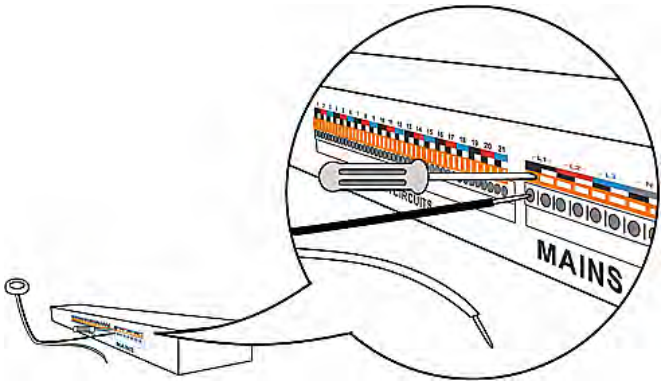


4. Strip the insulation of the CT leads around 0.6 mm from the end.
5. Connect the CT leads to the corresponding CT terminals on the Branch Circuit Monitor.
   a. Locate the BLACK (L1) channel in the MAINS channel group on the Branch Circuit Monitor.

      The channel comprises two CT terminals: the black one for connecting the CT's black lead and the white one for connecting the white lead. See ***Channel Convention*** (on page 6) for channel definitions.

   b. Use a small flat head screwdriver to press and hold down the orange button above the black CT terminal of this channel.
   c. Plug the CT's black lead into the black CT terminal.

Important: The CT lead's color must be identical to the color of the CT terminal where it is plugged.

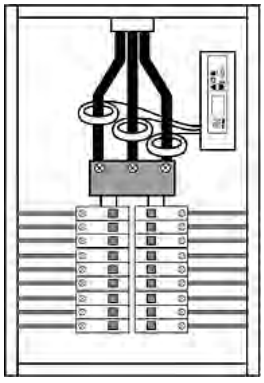


d. Release the orange button. Verify that the CT black lead is securely fastened.

e. Plug the CT's white lead into the "adjacent" white terminal of the same channel in the same manner.

6. Repeat the same steps to snap a mains CT onto the mains phase B conductor and connect the CT to the RED (L2) channel in the MAINS channel group on the Branch Circuit Monitor.

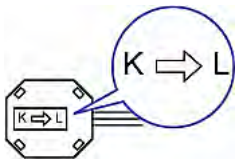
7. Repeat the same steps to snap a mains CT onto the mains phase C conductor and connect the CT to the BLUE (L3) channel in the MAINS channel group on the Branch Circuit Monitor.



Important: Do NOT plug any CT leads into the channel labeled N on the Branch Circuit Monitor because the Branch Circuit Monitor does not support measuring the neutral conductor.

Connecting Branch Circuit CTs

When snapping the CT onto a circuit conductor, make sure the CT's arrow mark points towards the load. For branch circuit CTs, the arrow mark is on the CT's bottom.



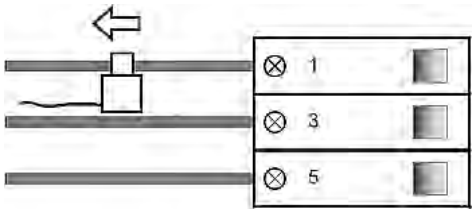
To connect branch circuit CTs:

1. Verify the single-phase or 3-phase branch circuit to monitor meets the maximum current rating specified for the BRANCH CIRCUITS channels on the Branch Circuit Monitor's nameplate or label.
2. Switch OFF the 1-pole or 3-pole circuit breaker(s) where the branch circuit CTs will monitor.

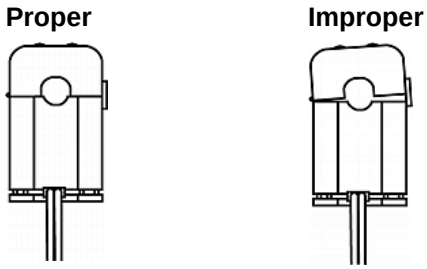
   Note: The Branch Circuit Monitor does not support measuring 2-pole branch circuit breakers so do not use the CT with a 2-pole breaker.

3. Open the CT by unlocking its release tab.

4. Slip the CT over a phase A conductor and snap it.
   - Make sure the direction of the arrow on the CT's bottom is the same as the following illustration.



   - Make sure the CT's release tab is locked properly.

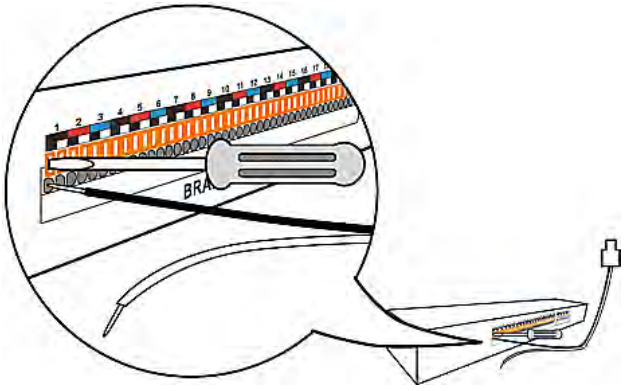


5. Strip the insulation of the CT leads around 0.6 mm from the end.
6. Connect the CT leads to the corresponding CT terminals on the Branch Circuit Monitor.
   a. Locate one of the black channels in the BRANCH CIRCUITS channel group on the Branch Circuit Monitor.

      The channel comprises two CT terminals: the black one for connecting the CT's black lead and the white one for connecting the white lead. See ***Channel Convention*** (on page 6) for channel definitions.

   b. Use a small flat head screwdriver to press and hold down the orange button above the black CT terminal of this channel.
   c. Plug the CT's black lead into the black CT terminal.

Important: The CT lead's color must be identical to the color of the CT terminal where it is plugged.

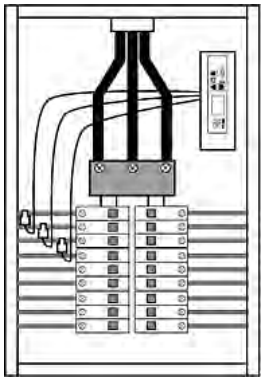


   d. Release the orange button. Verify that the CT black lead is securely fastened.
   e. Plug the CT's white lead into the "adjacent" white terminal of the same channel in the same manner.
7. Repeat the same steps to snap a branch circuit CT onto a phase B conductor, and connect the CT to one of the RED channels on the Branch Circuit Monitor.

- For a 3-phase branch circuit connection, the phase B CT must be connected to the red channel that is next to the black channel where the phase A CT is connected. For example, if the phase A CT is connected to the channel #4, the phase B CT must be connected to the channel #5.

8. Repeat the same steps to snap a branch circuit CT onto a phase C conductor, and connect the CT to one of the BLUE channels on the Branch Circuit Monitor.

   - For a 3-phase branch circuit connection, the phase C CT must be connected to the blue channel that is next to the red channel where the phase B CT is connected. For example, if the phase B CT is connected to the channel #5, the phase C CT must be connected to the channel #6.



9. To monitor additional branch circuits, repeat the above steps to snap branch circuit CTs onto other branch circuit conductors, and connect these CTs to the remaining channels on the Branch Circuit Monitor.

Configuring the Branch Circuit Monitor

There are two ways to initially configure a Branch Circuit Monitor device:

- Connect the Branch Circuit Monitor device to a computer to configure it, using a serial or USB connection between the Branch Circuit Monitor and the computer.

  The computer must have a communications program such as HyperTerminal or PuTTY.

  For a serial connection, you need a null-modem cable with DB9 connectors on both ends (Raritan part number: 254-01-0006-00).

- Connect the Branch Circuit Monitor device to a TCP/IP network that supports DHCP.

  The DHCP-assigned IP address can be retrieved through the Branch Circuit Monitor's MAC address. You can contact your LAN administrator for assistance. See ***MAC Address*** (on page 41).

  A Category 5e/6 UTP cable is required for a wired network connection.

Connecting the Branch Circuit Monitor to a Computer

To configure the Branch Circuit Monitor using a computer, it must be connected to the computer with an RS-232 serial interface. The computer must have a communications program such as HyperTerminal or PuTTY.

If your computer does not have a serial port, use a regular USB cable to connect the Branch Circuit Monitor to the computer for initial configuration. The Branch Circuit Monitor device can emulate a USB-to-serial converter after the USB-to-serial driver is properly installed in the Windows® operating system.

Note: Not all serial-to-USB converters work properly with the Branch Circuit Monitor device so this section does not introduce the use of such converters.

Now connect the Branch Circuit Monitor to a computer for initial configuration by following either of the following procedures.

To make a serial connection:

1. Connect one end of the null-modem cable to the RS-232 port labeled CONSOLE / MODEM on the Branch Circuit Monitor.
2. Connect the other end of the null-modem cable to the serial port (COM) on the computer.

To make a USB connection:

1. Connect one end of a regular USB cable to the USB-B port on the Branch Circuit Monitor.
2. Connect the other end of the USB cable to the USB-A port on the computer.

Installing the USB-to-Serial Driver

The Branch Circuit Monitor can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion Serial Console" is required for Microsoft® Windows® operating systems. Download the driver files, which include *dominion-serial.inf* and *dominion-serial-setup.exe*, from the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).

To install the driver in Windows® Vista and 7:

1. Disconnect the Branch Circuit Monitor's USB cable from the computer.
2. Run dominion-serial-setup.exe. A Dominion Serial Console Driver Setup Wizard appears.
3. Click Install to install the driver.

4. Click Finish when the installation is complete.
5. Connect the Branch Circuit Monitor's USB cable to the computer. The driver is automatically installed.

To install the driver in Windows® XP:

1. Disconnect the Branch Circuit Monitor's USB cable from the computer.
2. Check if the file "usbser.sys" is available in C:\Windows\ServicePackFiles\i386. If not, extract it from the Windows installation CD disc, and copy it to the same directory where the USB-to-serial driver is stored.
   - On a CD disc with SP3 included, it is extracted from I386\SP3.CAB.
   - On a CD disc with SP2 included, it is extracted from I386\SP2.CAB.
   - On a CD without an SP, it is extracted from I386\DRIVER.CAB.
3. Connect the Branch Circuit Monitor's USB cable to the computer.
4. The computer detects the new device and the "Found New Hardware Wizard" dialog appears. If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the Dominion Serial Console, and choose Update Driver.
5. Select "Install from a list or specific location," and specify the location where the driver is stored.
6. If you see the message requesting the file "usbser.sys," specify the location of the file.
7. The installation is complete.

In Linux:

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the Branch Circuit Monitor to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

> set line /dev/ttyACM0

> connect

Connecting the Branch Circuit Monitor to Your Network

To use the web interface to administer the Branch Circuit Monitor, you must connect the Branch Circuit Monitor to your local area network (LAN). The Branch Circuit Monitor can be connected to a wired or wireless network.

To make a wired connection:

1. Connect a standard Category 5e/6 UTP cable to the ETHERNET port on the Branch Circuit Monitor.
2. Connect the other end of the cable to your LAN.

To make a wireless connection:

Do one of the following:

- Plug a 802.11n wireless USB LAN adapter into the USB-A port on your Branch Circuit Monitor.
- Connect a USB docking station to the USB-A port on the Branch Circuit Monitor and plug the 802.11n wireless USB LAN adapter into the appropriate USB port on the docking station.

Supported Wireless LAN Configuration

If you select the wireless connection, ensure that both of your wireless USB LAN adapter and wireless network configuration meet the following requirements.

- Network type: 802.11n
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK
- Encryption: CCMP (AES)

Important: Currently only Raritan-provided wireless USB LAN adapters are supported. You may contact Raritan Technical Support for this information.

Initial Network Configuration

After the Branch Circuit Monitor device is connected to your network, you must provide it with an IP address and some additional networking information.

This section describes the initial configuration via a serial or USB connection.

Note: To configure the Branch Circuit Monitor via the LAN, see **Using the Web Interface** *(on page 43) for using the web interface.*

To configure the Branch Circuit Monitor device:

1. Go to the computer that you connected to the Branch Circuit Monitor and open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and make sure the port settings are configured as follows:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the Branch Circuit Monitor by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion Serial Console" under the Ports group.
3. Press Enter.
4. The Branch Circuit Monitor prompts you to log in. Note that both of user name and password are case sensitive.
   a. At the Username prompt, type `admin` and press Enter.
   b. At the Password prompt, type `raritan` and press Enter.
5. You are prompted to change the password if this is the first time you log in to the Branch Circuit Monitor. Follow the onscreen instructions to type your new password.
6. The # prompt appears when you log in successfully.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands, and press Enter. All commands are case sensitive.
   a. To set the networking mode, type this command:

```
network mode <mode>
```

where <mode> is either *wired* for wired connection (default) or *wireless* for wireless connection.

b. For the wired network mode, you may configure the LAN interface settings. In most scenarios, the default setting (auto) works well and should not be changed unless required.

To set	Use this command
LAN interface speed	`network interface LANInterfaceSpeed <option>` where <option> is *auto*, *10Mbps*, or *100Mbps*.
LAN interface duplex mode	`network interface LANInterfaceDuplexMode <mode>` where <mode> is *half*, *full* or *auto*.

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,
`network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

c. For the wireless network mode, you must configure the Service Set Identifier (SSID) parameter.

To set	Use this command
SSID	`network wireless SSID <ssid>` where <ssid> is the SSID string.

If necessary, configure more wireless parameters shown in the following table.

To set	Use this command
BSSID	`network wireless BSSID <bssid>` where <bssid> is the AP MAC address.

To set	Use this command
Authentication method	`network wireless authMethod <method>` where <method> is *psk* for Pre-Shared Key or *eap* for Extensible Authentication Protocol.
PSK	`network wireless PSK <psk>` where <psk> is the PSK string.
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` where <outer_auth> is *PEAP*.
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` where <inner_auth> is *MSCHAPv2*.
EAP identity	`network wireless eapIdentity <identity>` where <identity> is your user name for EAP authentication.
EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

Note: The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE."

d. To determine which IP protocol is enabled and which IP address returned by the DNS server is used, configure the following parameters.

To set	Use this command
IP protocol	`network ip proto <protocol>` where <protocol> is *v4Only* for enabling IPv4, *v6Only* for enabling IPv6 or *both* for enabling both IPv4 and IPv6 protocols.
Which IP address returned by the DNS server is used	`network ip dnsResolverPreference <resolver>` where <resolver> is *preferV4* for IPv4 addresses or *preferV6* for IPv6 addresses.

e. If you enabled the IPv4 protocol in the previous step, configure the IPv4 network parameters.

To set	Use this command
IP configuration method	`network ipv4 ipConfigurationMode <mode>` where <mode> is either *dhcp* for auto configuration (default) or *static* for specifying a static IP address.

- For the IPv4 DHCP configuration, configure this parameter.

To set	Use this command
Preferred host name (optional)	`network ipv4 preferredHostName <name>` where <name> is the preferred host name.

Tip: To override the DHCP-assigned IPv4 DNS servers with those you specify manually, type this command:

`network ipv4 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv4 commands for manually specifying DNS servers.

- For the static IPv4 configuration, configure these parameters.

To set	Use this command
Static IPv4 address	`network ipv4 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Subnet mask	`network ipv4 subnetMask <netmask>` where <netmask> is the subnet mask.
Gateway	`network ipv4 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv4 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv4 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

f. If you enabled IPv6 in the earlier step, configure the IPv6 network parameters.

To set	Use this command
IP configuration method	`network ipv6 ipConfigurationMode <mode>` where <mode> is either *automatic* for auto configuration (default) or *static* for specifying a static IP address.

Tip: To override the DHCP-assigned IPv6 DNS servers with those you specify manually, type this command:

`network ipv6 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv6 commands for manually specifying DNS servers.

- For the static IPv6 configuration, you should configure the following parameters. Note that the IP address must follow the IPv6 format.

To set	Use this command
Static IPv6 address	`network ipv6 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Gateway	`network ipv6 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv6 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv6 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

9. To quit the configuration mode with or without saving the changes, type either command, and press Enter.

Command	Description
`apply`	Save all configuration changes and quit the configuration mode.
`cancel`	Abort all configuration changes and quit the configuration mode.

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one. Current network settings are displayed.

Command	Description
`show network`	Show network parameters.
`show network ip all`	Show all IP configuration parameters.
`show network wireless details`	Show all wireless parameters. (Perform this command only when you enable the wireless mode.)

Tip: You can also type "`show network wireless`" to display a shortened version of wireless settings.

11. If all are correct, type `exit` to log out of the Branch Circuit Monitor. If any are incorrect, repeat Steps 7 to 10 to change any network settings.

The IP address configured may take seconds to take effect.

Mapping Channels with Branch Circuits

The best way to identify the branch circuit each channel is monitoring is to customize the channel names in the web interface. A hard copy worksheet documenting the use of each branch circuit is usually affixed to the electrical panel. It is strongly recommended to contain this worksheet information when assigning the channel names.

To map channels with monitored branch circuits:

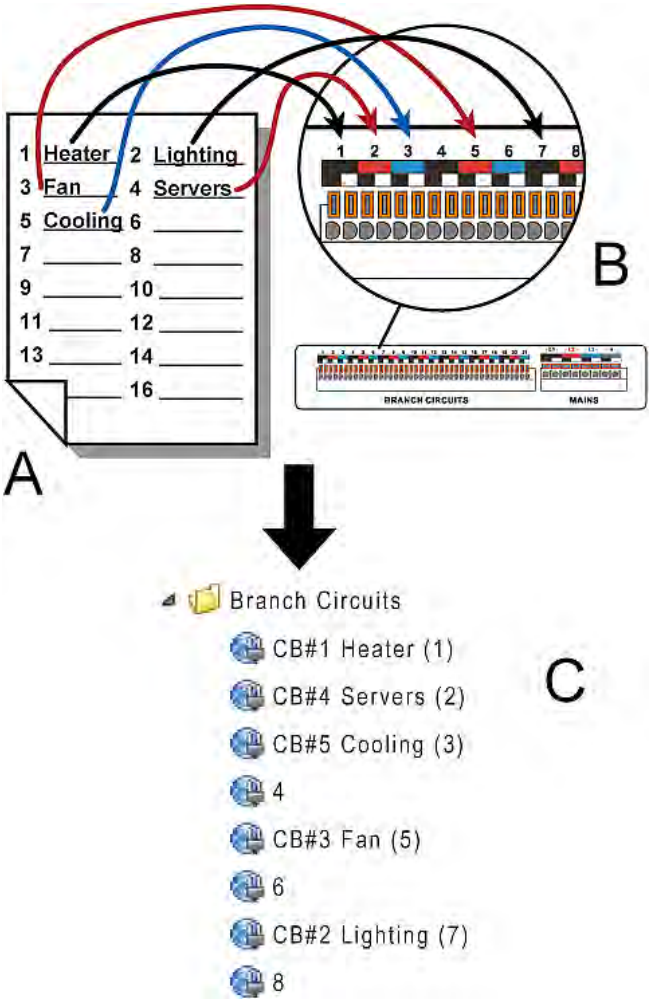
1. You should have noted down every branch circuit's panel number along with every CT's channel number in the procedure of ***Setting Up a Power Monitoring System*** (on page 7). If not yet, collect this information now.
2. Locate the electrical panel's worksheet, which is usually available on the panel's cover.
3. Log in to the web interface of the Branch Circuit Monitor. See ***Login*** (on page 44) in the User Guide.
4. Check which branch circuits are single-phase and which ones are 3-phase, and then configure them accordingly. See ***Configuring the Branch Circuit Channels*** (on page 77) in the User Guide.
5. Change the channel names according to the channel-mapping information collected in Step 1 and the panel's worksheet.
   a. Click the desired channel's icon in the left pane.

- When there are no names assigned, a channel shows its channel number only.
- For a 3-phase branch circuit, its channel number includes 3 numbers that are connected with a dash, such as 1-3, 4-6, 7-9, 10-12 and so on.

b. Click Setup in the right pane.

c. Type a name in the Name field. After assigning a channel name, the channel number is enclosed in parentheses, following the customized channel name.

Raritan suggests including both of the panel number and the branch circuit's use in the channel name. For example, if a CT attached to the branch circuit #2 (phase A) is connected to the channel #7 on the Branch Circuit Monitor and the worksheet indicates that the branch circuit #2 is used to power the lighting system, then you can name the channel 7 as "CB#2 Lighting."



Item	Description
A	Electrical panel's worksheet
B	Channels on the Branch Circuit Monitor
C	Channels shown in the web interface with customized channel names for channels #1, #2, #3, #5, and #7

Connecting Environmental Sensors (Optional)

To enable the detection of environmental factors around the Branch Circuit Monitor, connect one or more Raritan environmental sensors to the Branch Circuit Monitor device.

The maximum distance for all sensor cabling plugged into the product's sensor port should not exceed 30 meters/100 feet. Contact Raritan Technical Support if you have questions.

You can connect up to 16 environmental sensors to a Branch Circuit Monitor device by using a Raritan sensor hub.

Note that a Raritan environmental sensor usually contains more than one sensor. For example, a DPX-T2H2 counts as 4 sensors, and a DPX-T3H1 counts as 4 sensors.

Warning: For proper operation, wait for 15~30 seconds between each connection operation or each disconnection operation of environmental sensors.

To directly connect one or multiple environmental sensors:

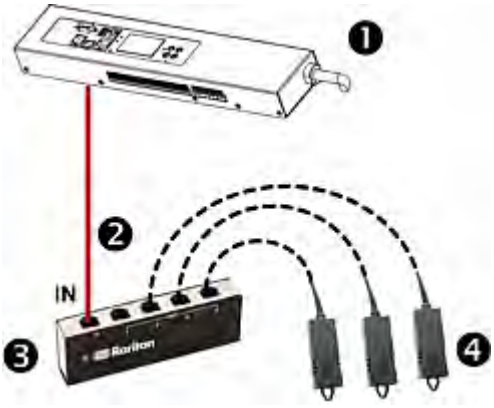
- Plug the connector of the environmental sensor into the SENSOR port on your Branch Circuit Monitor device.

  Note: Depending on the model you purchased, the total number of SENSOR ports varies.

To connect environmental sensors via an optional PX sensor hub:

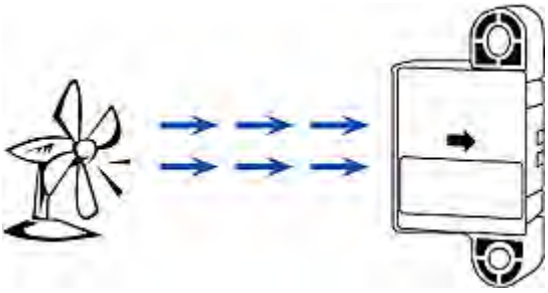
1. Connect a Raritan sensor hub to the Branch Circuit Monitor device.
   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
   b. Plug the other end into the SENSOR port on the Branch Circuit Monitor device.
2. Connect Raritan environmental sensors to any of the four OUT ports on the hub.

Raritan sensor hubs CANNOT be cascaded so at most a sensor hub can be connected to each SENSOR port on the Branch Circuit Monitor device. This diagram illustrates a configuration with a sensor hub connected.



❶	The Branch Circuit Monitor device
❷	Raritan-provided phone cable
❸	Raritan PX sensor hub
❹	Raritan environmental sensors

3. If there are any Raritan air flow sensors attached, make sure that sensor faces the source of the wind (such as a fan) in the appropriate orientation as indicated by the arrow on that sensor.



About Contact Closure Sensors

Raritan's contact closure sensor (DPX-CC2-TR) can detect the open-and-closed status of the connected detectors/switches. It requires the integration of at least a discrete (on/off) detector/switch to work properly. The types of discrete detectors/switches that can be plugged into DPX-CC2-TR include those for:

- Door open/closed detection
- Door lock detection
- Floor water detection
- Smoke detection
- Vibration detection

Raritan does NOT provide these discrete detectors/switches. They are third-party probes so you must test them with Raritan's DPX-CC2-TR to ensure they work properly.

Integration and testing for third-party detectors/switches is the sole responsibility of the customer. Raritan cannot assume any liability as a result of improper termination or failure (incidental or consequential) of third-party detectors/switches that customers provide and install. Failure to follow installation and configuration instructions can result in false alarms or no alarms. Raritan makes no statement or claim that all third-party detectors/switches will work with DPX-CC2-TR.

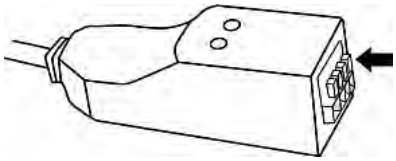
Connecting Third-Party Detectors/Switches to DPX-CC2-TR

A DPX-CC2-TR unit provides two channels for connecting two third-party detectors/switches. There are four spring-loaded termination points on the body of DPX-CC2-TR: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with another channel. You must plug the third-party detectors/switches into these termination points.

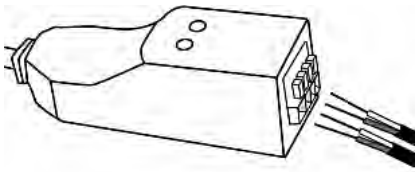
To connect third-party detectors/switches:

1. Strip the insulation around 12mm from the end of each wire of two third-party detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points on the body of DPX-CC2-TR.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both third-party detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of another detector/switch into the two termination points to the right.



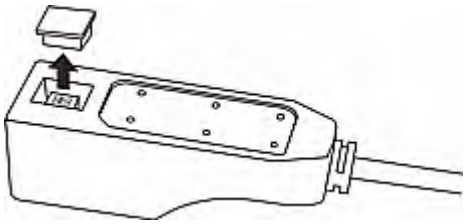
4. Release the tiny rectangular buttons after inserting the wires properly.
5. Verify that these wires are firmly fastened.

Configuring a Contact Closure Sensor

Before using DPX-CC2-TR to detect the contact closure status, water, smoke or vibration, you must determine the normal state by adjusting its dip switch, which controls the LED state on the body of DPX-CC2-TR. A dip switch is associated with a channel.

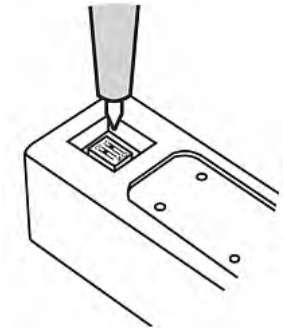
To adjust the dip switch setting:

1. Place the detectors/switches connected to DPX-CC2-TR to the position where you want to detect a specific environmental situation.
2. Uncover the dip switch on the body of DPX-CC2-TR.



3. To set the Normal state for channel 1, locate the dip switch labeled 1.
4. Use a pointed tip such as a pen to move the slide switch to the end labeled NO (Normally Open) or NC (Normally Closed).

- Normally Open: The open status of the connected detector/switch is considered normal.
- Normally Closed: The closed status of the connected detector/switch is considered normal. This is the default.



5. To set the Normal state for channel 2, repeat Step 4 for adjusting the other dip switch's setting.
6. Install back the dip switch cover.

Note: The dip switch setting must be properly configured, or the sensor LED may be incorrectly lit in the Normal state.

Contact Closure Sensor LEDs

DPX-CC2-TR is equipped with the LEDs for showing the state of the connected detectors/switches.

The LED is lit when the associated detector/switch is in the "abnormal" state, which is the opposite of the Normal state. See ***Configuring a Contact Closure Sensor*** (on page 29) for how to set the Normal state.

The meaning of a lit LED varies depending on the Normal state settings.

- **When the Normal state is set to Closed:**

LED	Sensor state
Not lit	Closed
Lit	Open

- **When the Normal state is set to Open:**

LED	Sensor state
Not lit	Open
Lit	Closed

How to Connect Differential Air Pressure Sensors

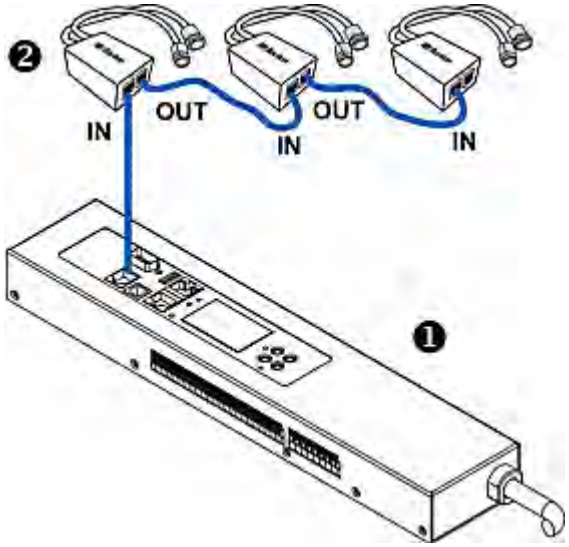
You can have a Raritan differential air pressure sensor connected to the Branch Circuit Monitor device if the differential air pressure data is desired.

With this sensor, the temperature around the sensor can be also detected through a temperature sensor implemented inside it.

To connect a differential air pressure sensor:

1. Plug one end of a Raritan-provided phone cable to the SENSOR port of the Branch Circuit Monitor device.
2. Plug the other end of this phone cable to the IN port of the differential air pressure sensor.

❶	The Branch Circuit Monitor device
❷	The Raritan differential air pressure sensor



Connecting a Logitech Webcam (Optional)

The Branch Circuit Monitor device supports the Logitech® QuickCam® Pro 9000 Webcam. After connecting this webcam, you can visually monitor the environmental condition near the Branch Circuit Monitor through the web interface from anywhere.

For more information on the webcam, see the user documentation accompanying that product.

To connect a webcam:

1. Connect the webcam to the USB-A port on the Branch Circuit Monitor device.
2. Position the webcam properly.
3. Reset or power cycle the Branch Circuit Monitor device.

Static images or videos captured by the webcam are immediately displayed in the Branch Circuit Monitor web interface. See ***Viewing the Webcam Images or Videos*** (on page 147).

Chapter 3 Panel Components

This chapter explains how to use the Branch Circuit Monitor. It describes the ports and channels on the device, and explains how to use the LCD display panel. The Branch Circuit Monitor comes with the following components on the outer panels.

- Line cord
- Connection ports
- LCD display
- Reset button
- Channels (terminals)

In This Chapter

Line Cord 33
Channels 34
Connection Ports 35
LCD Display Panel 36
Reset Button 42

Line Cord

The Branch Circuit Monitor contains a flexible cord containing the five wires for a 5-wire (3P+N+PE) AC connection. The cord is to be connected to a 3-phase branch circuit for electricity input. Make sure you switch OFF the breaker of the branch circuit that will power the Branch Circuit Monitor before connecting the cord.

Connect the Branch Circuit Monitor's line cord by following the procedure below:

a. Connect the L1 wire to a phase A connection point in the panel.

b. Connect the L2 wire to a phase B connection point in the panel.

c. Connect the L3 wire to a phase C connection point in the panel.

d. Connect the N wire to the panel's neutral bus.

e. Connect the GND wire to the panel's ground bus.

See the label or nameplate of your Branch Circuit Monitor model for appropriate input voltage ratings.

There is no power switch on the Branch Circuit Monitor. To power cycle it, power OFF the branch circuit breaker, wait 10 seconds and then power on the breaker.

Channels

A channel on the Branch Circuit Monitor is used to monitor a circuit, which may be phase A, B or C. There are two types of channel groups: MAINS and BRANCH CIRCUITS. MAINS channels are for monitoring the main circuits, and BRANCH CIRCUITS channels are for branch circuits. The maximum current ratings supported by different channel groups are different. See the nameplate or label affixed to your Branch Circuit Monitor for appropriate ratings supported by each channel group. For example, the BCM-2400 can monitor a mains rated at a maximum of 200A and 21 branch circuits rated at a maximum of 30A.

The total number of channels varies from model to model, and this number is included in the first numeric digits of the model name. For example, a BCM-2400 model can measure up to 24 circuits, including 21 branch circuits and 1 three-phase wye-connected mains (L1, L2 and L3).

The Branch Circuit Monitor uses both a number and a color to identify every channel. Three channel colors are available:

- Black: It is recommended using the black channel to monitor the phase A circuit.
- Red: It is recommended using the red channel to monitor the phase B circuit.
- Blue: It is recommended using the blue channel to monitor the phase C circuit.

For more information, see ***Channel Convention*** (on page 6).

Note: In the web interface, the black channel is called "Phase A," the red channel "Phase B," and the blue channel "Phase C."

Mains Channels

Mains channels are labeled MAINS on the Branch Circuit Monitor and are used to monitor the mains conductors. Their channel numbers are L1, L2 and L3.

Important: Do NOT plug any CT leads into the channel labeled N on the Branch Circuit Monitor because the Branch Circuit Monitor does not support measuring the neutral conductor.

L1 is the black channel, L2 the red channel, and L3 the blue channel.

See the nameplate or label affixed to your Branch Circuit Monitor for ratings supported by the MAINS channel groups.

Branch Circuit Channels

Branch circuit channels are labeled BRANCH CIRCUITS on the Branch Circuit Monitor and are used to monitor branch circuits. Their channel numbers are sequential numbers that start at 1.

The following lists the channel numbers of the black, red and blue channels:

- Black channels: 1, 4, 7, 10, 13, 16 and so on.
- Red channels: 2, 5, 8, 11, 14, 17 and so on.
- Blue channels: 3, 6, 9, 12, 15, 18 and so on.

See the nameplate or label affixed to your Branch Circuit Monitor for ratings supported by the BRANCH CIRCUITS channel groups.

CT Terminals and Buttons

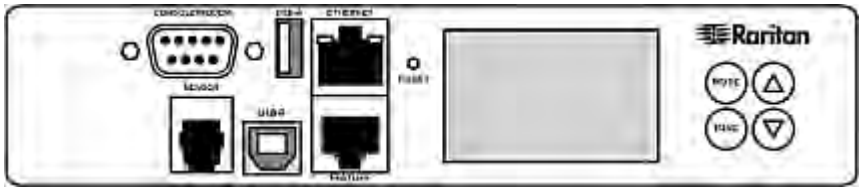
A channel comprises two CT terminals for connecting to one CT. A Raritan CT has two leads, which transmit different signals and are marked with different colors: black or white. Therefore, the CT terminals on the Branch Circuit Monitor are also marked with either the black or white color to identify which CT lead to connect.

Make sure the CT terminal's color matches the Raritan CT lead's color when plugging a CT lead, or the signals are reversed, resulting in incorrect measurement of power.

The tiny orange button above each CT terminal controls the spring inside the corresponding terminal. To plug a CT lead into a CT terminal or to unplug a CT lead from the terminal, first press and hold down the button above the corresponding terminal.

For more information, see ***Connecting Mains CTs*** (on page 9) or ***Connecting Branch Circuit CTs*** (on page 12).

Connection Ports



The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the Branch Circuit Monitor device.

Port	Used for...
	This port can be used for disaster recovery of the Branch Circuit Monitor device. Contact Raritan Technical Support for instructions.
USB-A	Connecting a USB device. This is a "host" port, which is powered, per USB 2.0 specifications.
FEATURE	Reserved for a future release. *Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.*
CONSOLE/ MODEM	Establishing a serial connection between a computer and the Branch Circuit Monitor device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the Branch Circuit Monitor device to the computer.
SENSOR	Connection to Raritan's environmental sensors. A Raritan sensor hub may be required if you want to connect more environmental sensors.
ETHERNET	Connecting the Branch Circuit Monitor device to your company's network: Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the Branch Circuit Monitor device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. *Note: Connection to this port is not required only when the Branch Circuit Monitor device is connected to a wireless network.*

LCD Display Panel

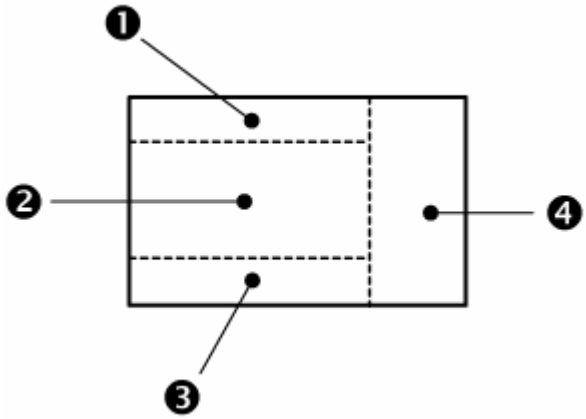
The LCD display panel shows different sensors' reading or status, and the device's MAC address.

It consists of:

- An LCD display
- Control buttons

LCD Display

Different types of information are shown in different sections of the LCD display. The diagram indicates the sections.



Section	Information shown
❶	Depending on your selection, the information displayed includes: • The selected "OUTLET" or "INLET." ▪ OUTLET: Refers to the branch circuit channel. For example, OUTLET 1 is the channel 1, OUTLET 2 is the channel 2, and so on. ▪ INLET: Refers to the mains channel so "INLET 1" is the mains. • The selected environmental sensor, including the sensor's ID number. For a sensor whose ID number is below 100, it is displayed as "SENSOR X" or "SENSOR XX," where X and XX are numeric digits.
❷	Depending on your selection, the information displayed includes: • Sensor reading comprising numeric digits or sensor state comprising alphabetical characters. • X, Y or Z coordinates of the selected environmental sensor. • Serial number of the selected environmental sensor. • MAC address of the Branch Circuit Monitor

❸	The text "ALARM" may appear to indicate either of the following scenarios: • For the branch circuit (OUTLET) and mains (INLET) channels, it means the displayed reading reaches or crosses the upper or lower thresholds if these thresholds have been enabled. • For a numeric environmental sensor, such as a temperature sensor, it means the sensor reading reaches or crosses the upper or lower thresholds if these thresholds have been enabled. • For a discrete (on/off) environmental sensor, such as a contact closure sensor, it means the sensor enters the abnormal state.
❹	The measurement unit for the selected sensor appears in this area. The measurement unit varies according to the sensor type: • A is displayed for the current reading. A means Amp. • V is displayed for the voltage reading. V means Volt. • W is displayed for the power reading. W means Watt. • % is displayed for a humidity sensor. • °C is displayed for a temperature sensor.

Control Buttons

There are four control buttons.

- Up and Down buttons for selecting a specific channel or ID number
- MODE button for switching between different types of target information, including mains (INLET) information, branch circuit (OUTLET) information, environmental sensor information, and MAC address
- FUNC button for switching between different types of data for a selected target, such as the current, voltage or power readings of a particular channel

Operating the LCD Display

By default the display panel shows the current reading of the first channel (that is, OUTLET 1) until you select a different channel or a different target.

Branch Circuit Information

The branch circuit information is displayed as "OUTLET" in the LCD display. By default the Branch Circuit Monitor displays the current reading of the channel 1 (that is, OUTLET 1) in the LCD display.

To display the branch circuit channel information:

1. Press the Up or Down button until the desired branch circuit channel number is displayed in the top of the LCD display. See ***LCD Display*** (on page 37).

   For example, OUTLET 3 is the channel #3, and OUTLET 20 is the channel #20.

   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.

2. Press the FUNC button to switch between voltage, active power and current readings of the selected branch circuit channel.

   - A is displayed for the current reading. A means Amp.
   - V is displayed for the voltage reading. V means Volt.
   - W is displayed for the power reading. W means Watt.

   If the text "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

If no button is pressed for tens of seconds, the LCD display returns to the current reading.

Mains Information

The mains information is displayed as "INLET" in the LCD display. Because there is only one mains channel group on the Branch Circuit Monitor, only "INLET 1" is available.

To display the mains channel information:

1. Press the MODE button until the term "INLET" is displayed. See ***LCD Display*** (on page 37).
2. Press the Up or Down button until the desired channel number of the mains is displayed in the bottom of the LCD display.

   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.

   L1 or L1-L2 is the mains channel labeled L1 on the Branch Circuit Monitor, L2 or L2-L3 is the channel labeled L2, and L3 or L3-L1 is the channel labeled L3.

3. Press the FUNC button to switch between voltage, active power and current readings of the selected mains channel.
   - A is displayed for the current reading. A means Amp.
   - V is displayed for the voltage reading. V means Volt.
   - W is displayed for the power reading. W means Watt.

   If the text "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

If no button is pressed for tens of seconds, the LCD display returns to the branch circuit (OUTLET) sensor reading.

Environmental Sensor Information

The environmental sensor information is displayed as "SENSOR" in the LCD display. Operate the LCD display to view information about the selected environmental sensor, including the sensor reading or state, X, Y, Z coordinates and its serial number.

To display the environmental sensor information:

1. Press the MODE button until the term "SENSOR" is displayed.
2. Press the Up or Down button until the desired environmental sensor's ID number is displayed in the top of the LCD display. See ***LCD Display*** (on page 37). For example, "SENSOR 1" refers to the #1 sensor listed on the External Sensors page of the web interface.
   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.
3. The LCD display shows the reading or state of the selected sensor in the middle of the LCD display.

   For a numeric sensor's reading, the appropriate measurement unit is displayed to the right of the reading.
   - % is displayed for a humidity sensor.
   - °C is displayed for a temperature sensor.

   For a discrete sensor, either of the following sensor states is displayed.
   - on: The sensor is in the abnormal state.
   - oFF: The sensor is in the normal state.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

4. Press the FUNC button to display the X, Y and Z coordinates of the sensor respectively.
   - X coordinate is shown as "x:XX," where XX are the first two numeric digits entered for the X coordinate in the web interface.
   - Y coordinate is shown as "y:XX," where XX are the first two numeric digits entered for the Y coordinate in the web interface.
   - Z coordinate is shown as "z:XX," where XX are the first two numeric digits entered for the Z coordinate in the web interface.

   If one or both of the first two digits for a specific coordinate are alphabetical characters, one or two underscores are displayed in place of the alphabetical characters.
5. Press the FUNC button again to display the serial number of the sensor, which is shown as "s:XX," where XX are two digits of the serial number. The LCD will cycle through the serial number from the first two digits to the final two.

   For example, if the serial number is AE17A00022, the LCD display shows the following information one after another:

   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

If no button is pressed for tens of seconds, the LCD display returns to the branch circuit (OUTLET) sensor reading.

MAC Address

The Branch Circuit Monitor's MAC address is available by operating the LCD display. Using commonly-used network tools, you can find this device's IP address via the MAC address. Contact your LAN administrator for assistance.

To display the MAC address:

1. Press the MODE button until the character "M" appears in the left side of the LCD display.
2. The MAC address is displayed as "M:XX", where XX are two digits of the MAC address. The LCD will cycle through the MAC address from the first two digits to the final two.

   For example, if the MAC address is 00:0d:5d:03:5E:1A, the LCD display shows the following information one after another:

   M:00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

Reset Button

The reset button is located inside a small hole which is labeled RESET.

The Branch Circuit Monitor device can be reset to its factory default values using this button when a serial connection is available. See ***Resetting to Factory Defaults*** (on page 304).

Without the serial connection, pressing this reset button restarts the Branch Circuit Monitor device's software.

Chapter 4 Using the Web Interface

This chapter explains how to use the web interface to administer a Branch Circuit Monitor.

In This Chapter

Supported Web Browsers....43
Logging in to the Web Interface....44
Logout....46
Introduction to the Web Interface....47
Viewing the Dashboard....58
Device Management....58
Channel Management....76
Setting Power Thresholds....83
User Management....88
Setting Up Roles....93
Access Security Control....95
Setting Up an SSL Certificate....107
Setting Up LDAP Authentication....112
Configuring Event Rules....118
Managing Event Logging....128
Viewing Connected Users....130
Monitoring Server Accessibility....131
Environmental Sensors....133
Copying Configurations with Bulk Configuration....143
Changing the Measurement Units....145
Viewing the Webcam Images or Videos....147
Network Diagnostics....147
Viewing the Communication Log....149
Downloading Diagnostic Information....150
Firmware Upgrade....150
Accessing the Help....153

Supported Web Browsers

The following web browsers can be used to access the Branch Circuit Monitor web interface:

- Internet Explorer® 7 (IE7) and Internet Explorer® 8 (IE8)
- Firefox 3.n.n (where n represents a numeric digit)
- Safari, Konqueror

Note: IE6 and Chrome are NOT supported.

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password. The first time you log in to the Branch Circuit Monitor, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

Exception: If you already changed the password for the admin account during the **Initial Network Configuration** *(on page 18), use the new password instead to log in to the web interface, and the Branch Circuit Monitor will NOT prompt you to change the password.*

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 88).

Login

The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

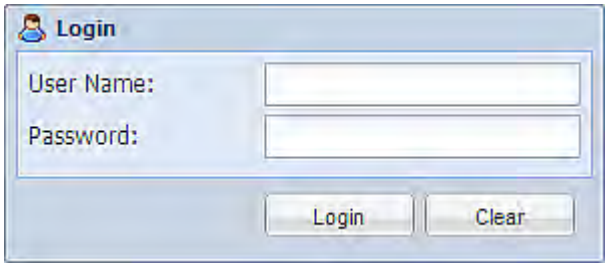
To log in to the web interface:

1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:

   http(s)://<ip address>

   where *<ip address>* is the IP address of the Branch Circuit Monitor device.

2. If any security alert message appears, click OK or Yes to accept. The Login page then opens.

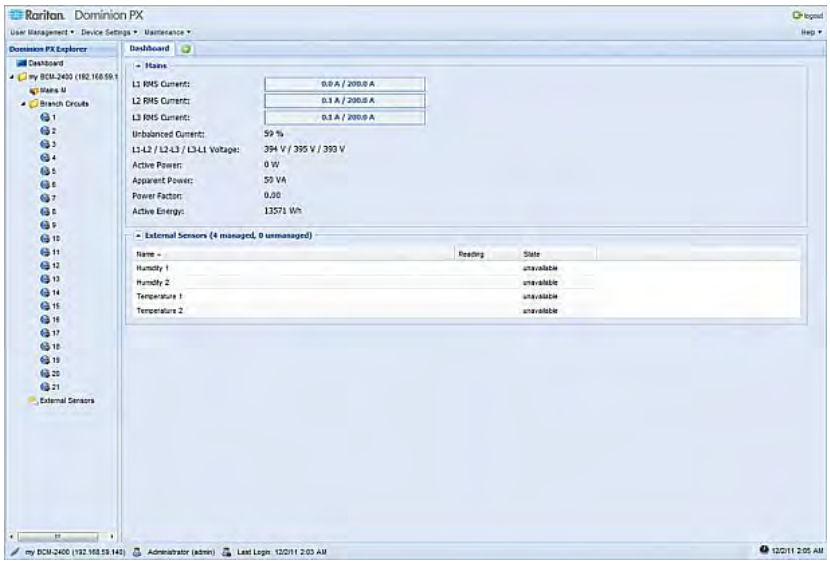


3. Type your user name in the User Name field, and password in the Password field.

   Note: Both the user name and password are case sensitive, so make sure you capitalize them correctly. If you typed them incorrectly, click Clear to clear either the inputs or any error message that appears.

4. Click Login or press Enter. The Branch Circuit Monitor page opens.

Note: Depending on your hardware configuration, elements shown on the Branch Circuit Monitor page may appear slightly different from this image.



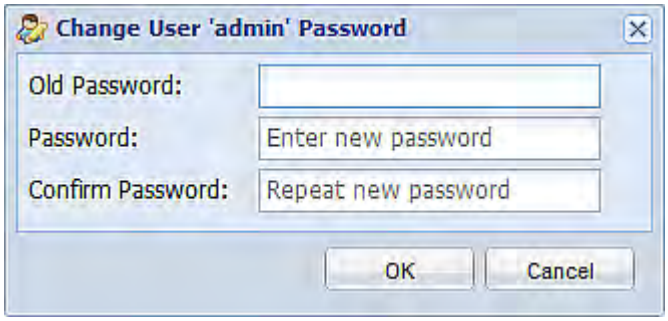
Changing Your Password

Normal users can change their own passwords if they have the Change Own Password permission. See ***Setting Up Roles*** (on page 93).

If you are the administrator (admin), the Branch Circuit Monitor web interface automatically prompts you to change the password if this is your first time to log in to the Branch Circuit Monitor.

To change your password:

1. Choose User Management > Change Password. The Change User 'XXX' Password dialog appears, where XXX is the user's login name.



2. Type the current password in the Old Password field.

3. Type your new password in the Password and Confirm Password fields. The password can be 4 to 32 characters long. It is case sensitive.
4. Click OK to save the changes.

Tip: If you have the Administrator Privileges, you can change other users' passwords. See **Modifying a User Profile** *(on page 91).*

Logout

After finishing your tasks with the Branch Circuit Monitor, you should log out to prevent others from accessing the web interface.

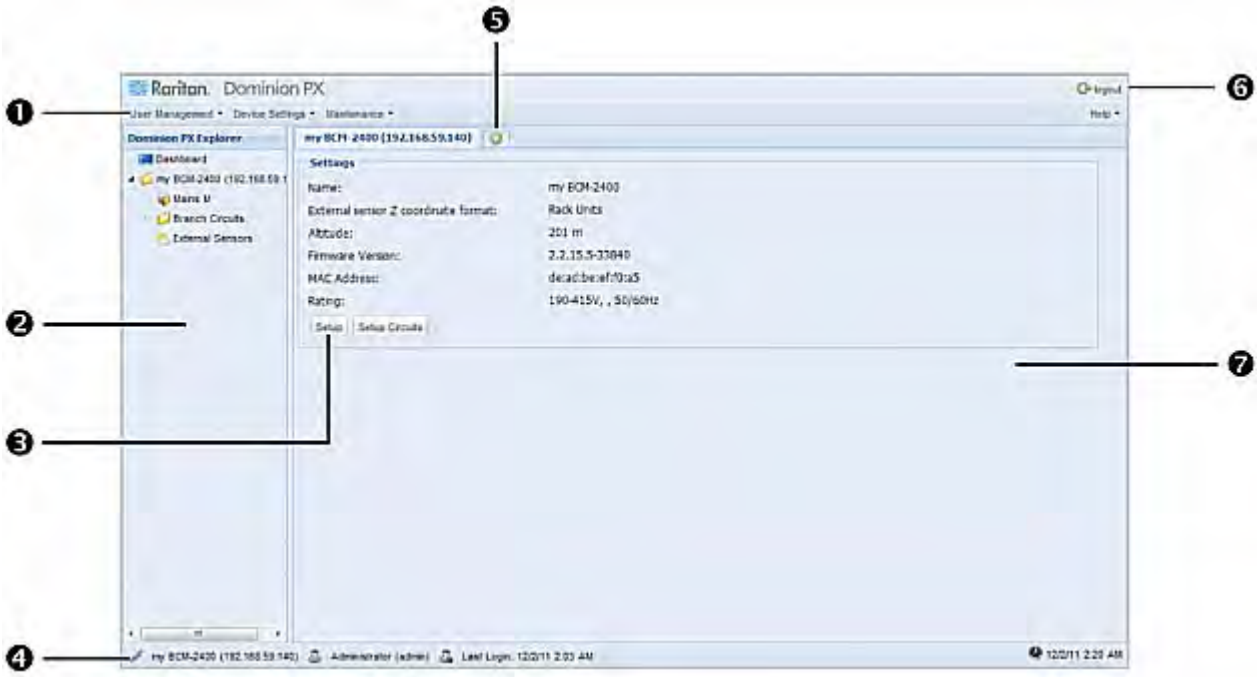
To log out of the web interface:

1. Do one of these:
   - Click "logout" on the top-right corner of the web interface.

   - Close the web browser by clicking the Close button ( ) on the top-right corner of the browser.
   - Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
   - Choose the Refresh command or click the Refresh button on the web browser.
2. Either the login page opens or the browser is closed, depending on your choice in the previous step.

Introduction to the Web Interface

The web interface provides two panes, a menu bar, a status bar, an Add Page icon, and a logout button throughout every page.



Number	Web interface element
❶	Menus
❷	Dominion PX Explorer pane
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button
❼	Data pane

* The Setup button is not available on some pages, such as the *Dashboard* page.

For detailed information about these web interface elements, see the sections that follow.

Menus

There is a menu bar across the top of the page. You can click any menu to select the desired menu item from the drop-down list.

Four menus are available for managing different tasks or showing information.

- **User Management** contains menu items for managing user profiles, permissions (roles), and password.
- **Device Settings** deals with device-related settings, such as the device name, network settings, security settings, and system time.
- **Maintenance** provides tools that are helpful for maintaining the Branch Circuit Monitor, such as the event log, hardware information, firmware upgrade and so on.
- **Help** displays information regarding the firmware and all open source packages embedded on the Branch Circuit Monitor. In addition, you can access the user guide from this menu.

Dominion PX Explorer Pane

The hierarchical tree to the left displays the Branch Circuit Monitor you are accessing as well as all physical components connected to or associated with this device, such as mains channels, branch circuit channels, and environmental sensors. In addition, an icon named Dashboard is available for displaying the device's summary information.

The tree structure comprises three hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
BCM folder*	Mains M	None
	Branch Circuits folder	1 to n**
	External Sensors folder	A list of connected environmental sensors
	Webcam***	None

* The BCM folder is named "my PX" by default. The name changes after customizing the device name. See ***Naming the Branch Circuit Monitor*** (on page 60).

** n represents the final number of that component.

*** A Webcam icon appears only when a Logitech® QuickCam® Pro 9000 Webcam is connected to the Branch Circuit Monitor. See ***Connecting a Logitech Webcam (Optional)*** (on page 32).

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

To navigate through the tree:

1. To expand any folders, see ***Expanding the Tree*** (on page 49).
2. To show any tree item's data, click on that item. See ***Add Page Icon*** (on page 52).

Expanding the Tree

The icons representing all components connected to or associated with the Branch Circuit Monitor are expanded by default. If they are hidden, you may expand the tree manually to show all component icons.

To expand the tree:

1. By default, the BCM folder has been expanded.

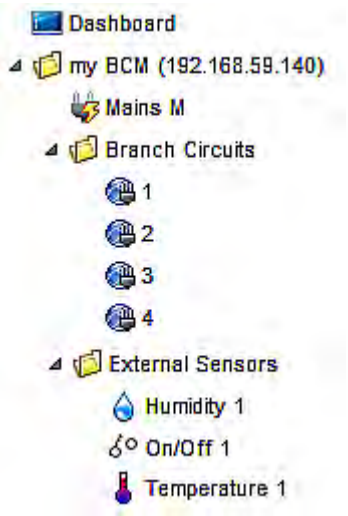
   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

   If it is not expanded, click the white arrow ▷ prior to the folder icon, or double-click the folder. The arrow then turns into a black, gradient arrow ◢, and icons of components or component groups appear below the BCM folder.

2. To expand any component group at the second level, click the white arrow ▷ prior to the folder icon, or double-click the folder.

   The arrow then turns into a black, gradient arrow ◢, and icons representing individual components appear below the group folder.

3. Repeat Step 2 for other component groups you want to expand. The expanded tree looks similar to this image.



Note: A Webcam icon appears only when a Logitech® QuickCam® Pro 9000 Webcam is connected to the Branch Circuit Monitor. See **Connecting a Logitech Webcam (Optional)** *(on page 32).*

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

Collapsing the Tree

You can collapse the whole tree structure or a specific component group to hide all or partial tree items.

To collapse the whole tree:

- Click the black, gradient arrow ◢ prior to the BCM folder icon, or double-click the folder.

Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

The arrow then turns into a white arrow ▷, and all items below the BCM folder disappear.

To hide some tree items:

1. Click the black, gradient arrow ◢ prior to the component group folder that you want to collapse, or double-click the folder.

The arrow then turns into a white arrow ▷, and all items below the folder disappear.

2. Repeat Step 1 for other component groups you want to collapse.

Adjusting the Pane

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the right border of the Dominion PX Explorer pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

Setup Button

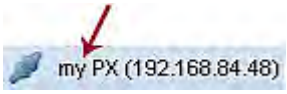
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

The status bar shows five pieces of information from left to right.

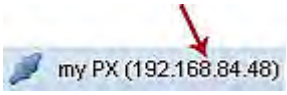
- **Device name:**

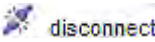
  This is the name assigned to the Branch Circuit Monitor device. The default is "my PX." See ***Naming the Branch Circuit Monitor*** (on page 60).



- **IP address:**

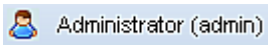
  The numbers enclosed in parentheses is the IP address assigned to the Branch Circuit Monitor device. See ***Initial Network Configuration*** (on page 18) or ***Modifying the Network Settings*** (on page 62).



Tip: The presence of the device name and IP address in the status bar indicates the connection to the Branch Circuit Monitor device. If the connection is lost, it shows "  *" instead.*

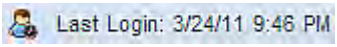
- **Login name:**

  This is the user name you used to log in to the web interface.



- **Last login time:**

  This shows the date and time this login name was used to log in to this Branch Circuit Monitor device last time.



  When the mouse pointer hovers over the last login time, detailed information about the last login is displayed, including the access client and IP address.

  For the login via a serial connection, <local> is displayed instead of an IP address.

  There are different types of access clients:

  - Web GUI: Refers to the Branch Circuit Monitor web interface.
  - CLI: Refers to the command line interface (CLI).
    The information in parentheses following "CLI" indicates how this user was connected to the CLI.
    - *Serial*: Represents the local connection (serial or USB).
    - *SSH*: Represents the SSH connection.
    - *Telnet*: Represents the Telnet connection.

- **System date and time:**

  Current date, year, and time are displayed to the right of the bar. If positioning the mouse pointer over the system date and time, the time zone information is also displayed.

Sometimes a flag icon ( ) may appear to the far right of the bar when a communication error between the Branch Circuit Monitor device and the graphical user interface (GUI) occurs. When the icon appears, you can click the icon to view the communications log. See ***Viewing the Communication Log*** (on page 149).

Add Page Icon

The Add Page icon , located on the top of the data pane, lets you open data pages of multiple tree items without overriding any opened page.

To open new data pages:

1. Click the Add Page icon . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.
3. To open more data pages, repeat Steps 1 to 2. All tabs representing opened pages are shown across the top of the page.

The following diagram shows a multi-tab example.

4. With multiple pages opened, you can take these actions:
   - To switch to one of the opened data pages, click the corresponding tab.

     If there are too many tabs to be all shown, two arrows (and) appear at the left and right borders of the pane. Click either arrow to navigate through all tabs.
   - To close any data page, click the Close button ( ) on the corresponding tab.

Logout Button

Click the logout button when you want to log out of the web interface.

Data Pane

The right pane shows the data page of the selected tree item. The data page includes the item's current status, settings and a Setup button (if available).

All tabs above the pane represent the opened data pages. The highlighted tab indicates the current selection.

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

More Information

This section explains additional web interface elements or operations that are useful.

Warning Icon

If the value you entered in a specific field is invalid, a red warning icon appears to the right and the field in question is surrounded by a red frame as shown in this illustration.

When this occurs, position your mouse pointer over the warning icon to view the reason and modify the entered value accordingly.

The Yellow- or Red-Highlighted Reading

When a numeric sensor's reading crosses any upper or lower threshold, the background color of the whole row turns to yellow or red for alerting users.

For a discrete (on/off) sensor, the row changes the background color when the sensor enters the abnormal state.

See the table for the meaning of each color:

Color	State
White	The background is white in one of the following scenarios: • For a numeric sensor, no thresholds have been enabled. • If any thresholds have been enabled for a numeric sensor, the sensor reading is between the lower and upper warning thresholds. • For a discrete (on/off) sensor, the sensor state is normal. • The sensor reading or state is unavailable.
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.
Red	The meaning of the red color varies depending on the sensor type: • For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold. • For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state.

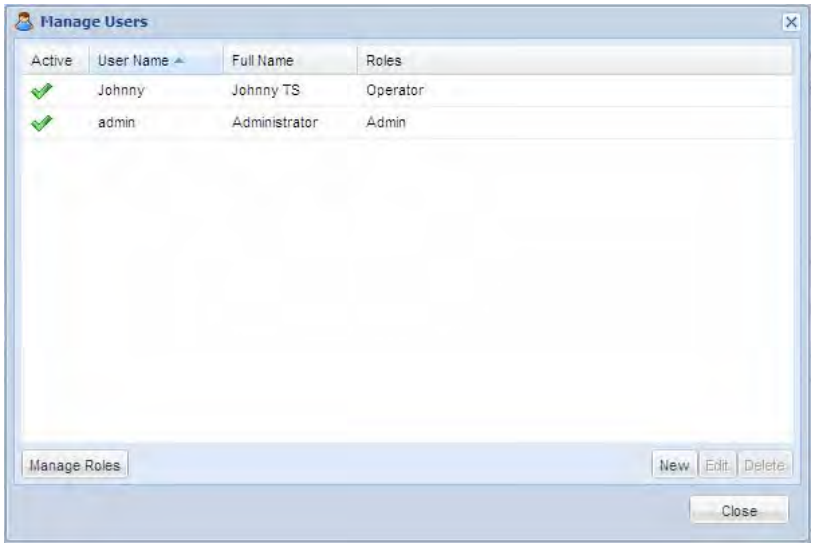
To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- below lower critical: The numeric sensor's reading drops below the lower critical threshold.
- below lower warning: The numeric sensor's reading drops below the lower warning threshold.
- above upper critical: The numeric sensor's reading reaches or exceeds the upper critical threshold.
- above upper warning: The numeric sensor's reading reaches or exceeds the upper warning threshold.
- alarmed: The discrete sensor is NOT in the normal state.

For information on the thresholds, see ***Setting Power Thresholds*** (on page 83).

Changing the View of a List

Some dialogs or data pages contain a list or table, such as the Manage Users dialog shown below. You may change the number of displayed columns or re-sort the list for better viewing the data. Note the column or sorting changes are not saved when quitting the dialog or data page. Next time when the dialog or page re-opens, the list returns to the default view.



Note: Not all dialogs support the sorting or column change functions.

Changing the Column

You can hide some columns of a list or table, or adjust a specific column's width.

To change displayed columns:

1. Hover your mouse pointer over any column header. A black triangle appears to the far right of this column header.
2. Click the black triangle, and a drop-down menu appears.
3. Point to Columns. A submenu showing all columns appears.
4. Click any column you want to deselect or select.
   - To hide a column, have its checkbox deselected.
   - To show a column, have its checkbox selected.

To change the column width:

1. Hover the mouse pointer to the right border of the desired column.
2. When the mouse pointer turns to a two-way arrow, drag the border horizontally to widen or shrink the column.

Changing the Sorting

By default, a list or table is sorted against the first column in the ascending order. You can re-sort the list in a reverse order or against a different column.

To re-sort the list by doing either of the following:

- Click the column header against which you want to sort the list.
  a. The first click sorts the list in the ascending order, indicated by a blue upward-pointing triangle ▲.
  b. The second click reverses the sorting to the descending order, indicated by a blue downward-pointing triangle ▼.
- Select a sorting command from the column menu.
  a. Hover your mouse pointer over the column header against which you want to sort the list. A black triangle appears to the far right of this column header.
  b. Click the black triangle, and a drop-down menu appears.
  c. Select Sort Ascending or Sort Descending.

The newly selected column header is marked with the upward- or downward-pointing triangle.

Resizing a Dialog

Most dialogs cannot be resized except for a few ones (such as the Event Log dialog), which can be resized to display more information at a time.

To resize a dialog:

1. Hover your mouse pointer over any border of the dialog.
2. When the mouse pointer turns to a double-headed arrow, drag the border vertically or horizontally to make the dialog bigger or smaller.

Browser-Defined Shortcut Menu

A shortcut menu, which is built in the web browser, may appear when right-clicking anywhere in the Branch Circuit Monitor web interface.

The shortcut menu functions are defined by the browser. For example, the Back command on the Internet Explorer® (IE) shortcut menu works the same as the Back button in the IE browser. Both of these functions take you to the previous page.

For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

Below is the illustration of the IE browser's shortcut menu. Available menu commands or items may slightly differ based on your web browser version.

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the Branch Circuit Monitor device's status.

The page is divided into various sections according to the component type, such as Mains and External Sensors.

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** *(on page 54).*

After clicking any other icon in the hierarchical tree, the Dashboard page is overridden. To return to the Dashboard page, click the Dashboard icon.

When the Dashboard page is opened, you can do the following to uncover or hide specific data.

To collapse any section:

1. Locate the section you want to collapse.
2. Click the upward arrow prior to the section title. The data specific to the section is hidden.

To expand a collapsed section:

1. Locate the section you want to expand.
2. Click the downward arrow prior to the section title. The data specific to the section appears.

Device Management

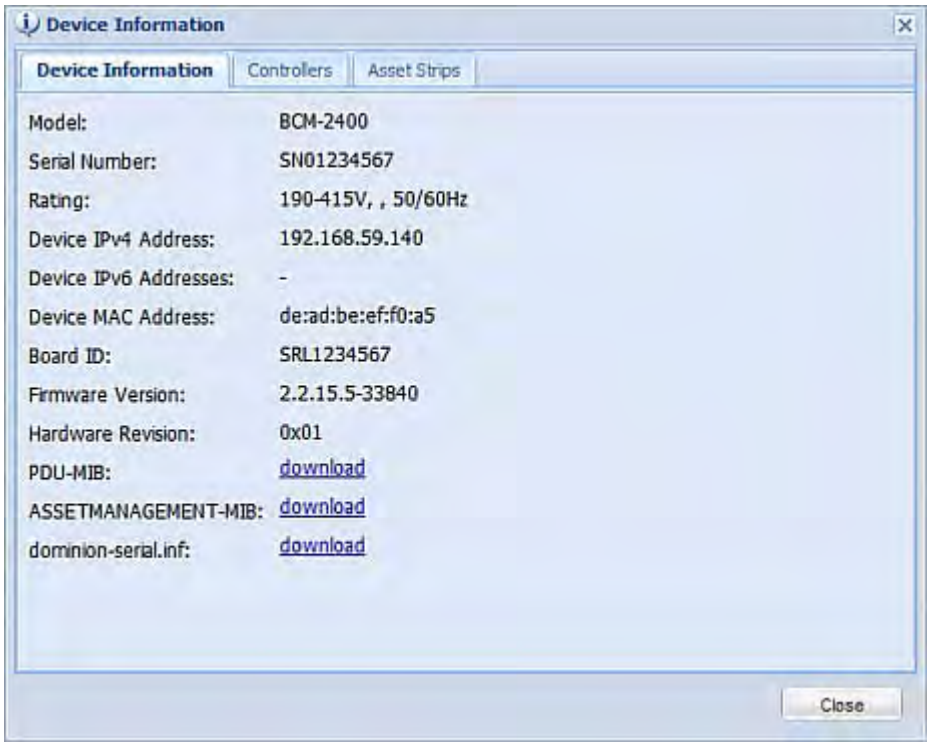
Using the web interface, you can retrieve basic hardware and software information, give the Branch Circuit Monitor a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying the Device Information

To display information specific to the Branch Circuit Monitor that you are using, such as its serial number, model name and rating, trigger the Device Information dialog.

To display the device information:

1. Choose Maintenance > Device Information. The Device Information dialog appears.



2. Click the tab containing the information you want to view.

Tab	Information shown
Device Information	General device information, such as model name, serial number, firmware version, hardware revision, and so on.
Controllers	The device controller's information, including its serial number, firmware version, and hardware revision.

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

3. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 57).

4. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 55).
5. Click Close to quit the dialog.

Tip: The firmware version is also available by clicking the BCM folder in the Dominion PX Explorer pane.

Naming the Branch Circuit Monitor

The default name for Branch Circuit Monitor is *my PX*. You may give it a unique device name.

To change the device name:

1. Click the BCM folder.

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Setup in the Settings section. The BCM Setup dialog appears.
3. Type a new name in the Device Name field.
4. Click OK to save the changes.

Modifying the Network Configuration

The network settings you can change via the web interface include wired, wireless, IPv4 and/or IPv6 settings.

Modifying the Network Interface Settings

The Branch Circuit Monitor supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See ***Connecting the Branch Circuit Monitor to Your Network*** (on page 17).

Wired Network Settings

The LAN interface speed and duplex mode were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 18).

By default, the LAN speed and duplex mode are set to "Auto" (automatic), which works in nearly all scenarios. You can change them if there are special local requirements.

To modify the network interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.

2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.
   - Auto: System determines the optimum LAN speed through auto-negotiation.
   - 10 Mbit/s: The LAN speed is always 10 Mbps.
   - 100 Mbit/s: The LAN speed is always 100 Mbps.
5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.
   - Auto: The Branch Circuit Monitor selects the optimum transmission mode through auto-negotiation.
   - Full: Data is transmitted in both directions simultaneously.
   - Half: Data is transmitted in one direction (to or from the Branch Circuit Monitor device) at a time.
6. Click OK to save the changes.

Tip: You can check the LAN status in the Current State field, including the speed and duplex mode.

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 18). You can change them via the web interface.

To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the Branch Circuit Monitor device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See ***Connecting the Branch Circuit Monitor to Your Network*** (on page 17).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

Note: BSSID refers to the MAC address of an access point in the wireless network.

7. In the Authentication field, click the drop-down arrow, and select an appropriate option from the list.

Option	Description
No Authentication	Select this option when no authentication data is required.
PSK	A Pre-Shared Key is required for this option. ▪ In the Pre-Shared Key field, type the PSK string.
EAP - PEAP	PEAP stands for Protected Extensible Authentication Protocol. The following authentication data is required: ▪ Inner Authentication: Only Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) is supported, allowing authentication to databases that support MSCHAPv2. ▪ Identity: Type your user name for EAP authentication. ▪ Password: Type your password for EAP authentication. ▪ CA Certificate: A third-party CA certificate must be provided for EAP authentication. Click Browse to select a valid certificate file. - To view the contents of the selected certificate file, click Show. - If the selected certificate file is invalid, click Remove. Then select a new file.

8. Click OK to save the changes.

Modifying the Network Settings

The Branch Circuit Monitor was configured for network connectivity during the installation and configuration process. See ***Configuring the Branch Circuit Monitor*** (on page 14). If necessary, you can modify any network settings using the web interface.

Selecting the Internet Protocol

The Branch Circuit Monitor device supports two types of Internet protocols -- IPv4 and IPv6. You can enable either or both Internet protocols. After enabling the desired Internet protocol(s), all but not limited to the following protocols will be compliant with the enabled Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

To select the appropriate Internet Protocol:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IP Protocol tab.
3. Select one checkbox according to the Internet protocol(s) you want to enable:
   - IPv4 only: Enables IPv4 only on all interfaces. This is the default.
   - IPv6 only: Enables IPv6 only on all interfaces.
   - IPv4 and IPv6: Enables both IPv4 and IPv6 on all interfaces.
4. If you selected the "IPv4 and IPv6" checkbox in the previous step, you must determine which IP address is used when the DNS resolver returns both of IPv4 and IPv6 addresses.
   - IPv4 Address: Use the IPv4 addresses returned by the DNS server.
   - IPv6 Address: Use the IPv6 addresses returned by the DNS server.
5. Click OK to save the changes.

Modifying the IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See ***Selecting the Internet Protocol*** (on page 63).

To modify the IPv4 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.

2. Click the IPv4 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
DHCP	To auto-configure the Branch Circuit Monitor, select DHCP. With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Netmask ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor only uses the primary IPv4 and IPv6 DNS servers.

Modifying the IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See ***Selecting the Internet Protocol*** (on page 63).

To modify the IPv6 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IPv6 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
Automatic	To auto-configure Branch Circuit Monitor, select Automatic. With this option selected, you can enter a preferred host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor only uses the primary IPv4 and IPv6 DNS servers.

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the Branch Circuit Monitor may fail to connect to the given host.

Therefore, DNS server settings are important for LDAP authentication. With appropriate DNS settings, the Branch Circuit Monitor can resolve the LDAP server's name to an IP address for establishing a connection. If the *SSL encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on LDAP authentication, see ***Setting Up LDAP Authentication*** (on page 112).

Modifying the Network Service Settings

The Branch Circuit Monitor supports these network communication services: HTTPS, HTTP, Telnet and SSH.

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the ***command line interface*** (see "***Using the Command Line Interface***" on page 161).

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

In addition, the Branch Circuit Monitor also supports the SNMP protocol.

Changing the HTTP(S) Settings

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the Branch Circuit Monitor device so it is a more secure protocol than HTTP.

By default, any access to the Branch Circuit Monitor device via HTTP is automatically redirected to HTTPS. See ***Forcing HTTPS Encryption*** (on page 96).

To change the HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.
2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

Warning: Different network services cannot share the same TCP port.

3. Click OK to save the changes.

Changing the SSH Settings

You can enable or disable the SSH access to the command line interface, or change the default TCP port for the SSH service. In addition, you can decide to log in using either the password or the public key over the SSH connection.

To change the SSH service settings:

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the SSH application, select the Enable SSH checkbox. To disable it, deselect the checkbox.
4. To select a different authentication method, select one of the checkboxes.
   - Allow password authentication only: Enables the password-based login only.
   - Allow public key authentication only: Enables the public key-based login only.
   - Allow password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click OK to save the changes.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 88).

Changing the Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the default TCP port for the Telnet service.

To change the Telnet service settings:

1. Choose Device Settings > Network Services > Telnet. The Telnet Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the Telnet application, select the Enable Telnet Access checkbox. To disable it, deselect the checkbox.

4. Click OK to save the changes.

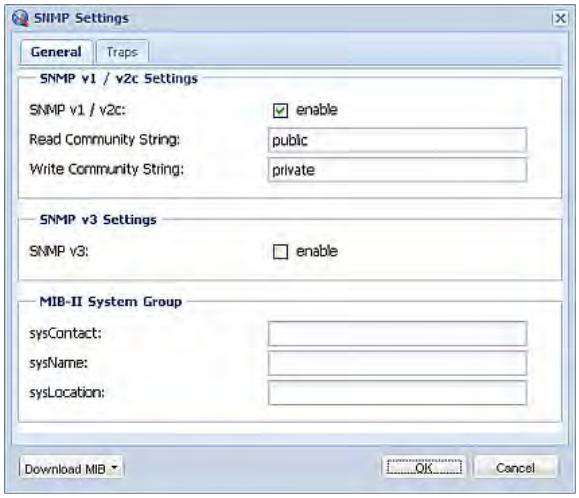
Configuring the SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the Branch Circuit Monitor device. Enabling SNMP communication allows the manager to retrieve the status of the Branch Circuit Monitor device.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Trap Rule" is enabled and the trap destination has not been set yet. See ***Configuring Event Rules*** (on page 118).

To configure the SNMP communication:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
   - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

   Tip: You can permit or disallow a user to access the Branch Circuit Monitor via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 156).*
4. Type the SNMP MIB-II sysContact value in the sysContact field.

5. Type the SNMP MIB-II sysName value in the sysName field.
6. Type the SNMP MIB-II sysLocation value in the sysLocation field.
7. Click OK to save the changes.

Important: You must download the SNMP MIB for your Branch Circuit Monitor to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see *Downloading SNMP MIB* (on page 158).

To configure SNMP trap destinations:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click the Traps tab.
3. Select the Enabled checkbox in the "System Snmp Trap Event Rule" field.
4. Specify the SNMP trap destinations by doing the following:
   a. You can specify up to 3 SNMP trap destinations in the Host *x* fields, where *x* is a number between 1 and 3.
   b. Specify a port number for each destination in the Port *x* fields, where *x* is a number between 1 and 3.
   c. Specify a community string for each destination in the Community *x* fields, where *x* is a number between 1 and 3.
5. Click OK to save the changes.

Tip: The SNMP trap destination settings can be also set in the Event Rule Settings dialog. See **Modifying an Action** *(on page 127).*

Setting the Date and Time

You can set the internal clock on the Branch Circuit Monitor device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for the Branch Circuit Monitor.

To set the date and time:

1. Choose Device Settings > Date/Time. The Configure Date/Time Settings dialog appears.
2. In the Time Zone field, click the drop-down arrow, and select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

   If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.
4. Choose one of the methods to set the date and time:

- To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
  - To set the date, delete existing numbers in the Date field and type new ones, or click the calendar icon to select a date. See ***How to Use the Calendar*** (on page 71) for details.
  - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on. You can enter the time by deleting existing numbers and typing new ones in the hour, minute and second fields, or clicking the arrows to adjust each number.
- To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.
  - To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
  - To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

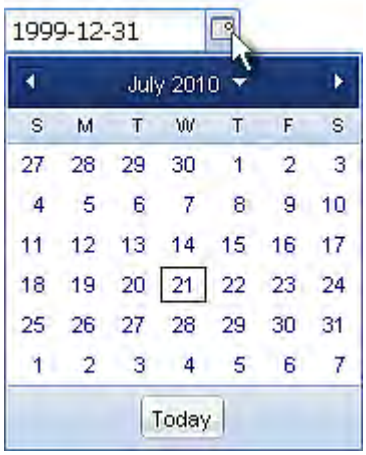
Note: If the Branch Circuit Monitor device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.

5. Click OK to save the changes.

Important: If you are using Raritan's Power IQ to manage the Branch Circuit Monitor, you must configure Power IQ and the Branch Circuit Monitor to have the same date/time or NTP settings.

How to Use the Calendar

The calendar icon next to the Date field is a convenient tool to quickly change the year, month and date.



To select a date using the calendar:

1. To change the year shown in the calendar, do either of the following:
   - Press Ctrl+Up arrow or Ctrl+Down arrow to switch between years.
   - Click , which is adjacent to the year, to show a list of years and months. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click or to show additional years.

2. To change the month shown in the calendar, do one of the following:
   - Press Ctrl+Right arrow or Ctrl+Left arrow to switch between months.
   - Click or on the top of the calendar to switch between months.

- Click , which is adjacent to the year, to show a list of years and months. Select the desired month from the list to the left and click OK.

3. To select a date, click that date on the calendar.
   - Click Today if you want to select today.

Note: On the calendar, the date for today is marked with a red frame.

Specifying the Device Altitude

You must specify the Branch Circuit Monitor device's altitude above sea level if a Raritan differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 315).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See ***Changing the Measurement Units*** (on page 145).

To specify the altitude of the Branch Circuit Monitor device:

1. Click the BCM folder.

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Setup in the Settings section. The BCM Setup dialog appears.
3. Type an integer number in the Altitude field. Depending on the measurement unit displayed, the range of valid numbers differs.
   - For meters (m), the value ranges between 0 and 3000.
   - For feet (ft), the value ranges between 0 and 9842.
4. Click OK to save the changes.

Setting Data Logging

The Branch Circuit Monitor can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the Branch Circuit Monitor's internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The Branch Circuit Monitor's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 155) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is disabled. Only users having the "Administrator" or "Change Data Logging Settings" permissions can enable or disable this feature. See ***Setting Up Roles*** (on page 93).

▶ **To configure the data logging feature:**

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All in Page to have all sensors selected.
5. Click OK to save the changes.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the Branch Circuit Monitor in Step 4, it is NOT recommended and this capability may be removed in the future.

Configuring the SMTP Settings

The Branch Circuit Monitor can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

Note: See **Configuring Event Rules** *(on page 118) for information on creating event rules to send email notifications.*

To set the SMTP server settings:

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the Number of Sending Retries field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:
   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
9. Click OK to save the changes.
10. Check if the recipient(s) receives the email successfully.

Setting the EnergyWise Configuration

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the Branch Circuit Monitor device so that this device becomes part of the Cisco EnergyWise domain.

The Cisco EnergyWise feature implemented on the Branch Circuit Monitor is disabled by default.

To set the Cisco EnergyWise configuration:

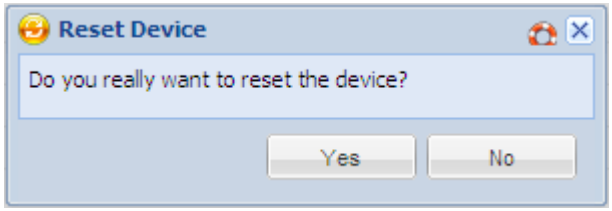
1. Choose Device Settings > EnergyWise. The EnergyWise Configuration dialog appears.
2. In the Enable EnergyWise field, select the "enable" checkbox to enable the Cisco EnergyWise feature.
3. In the "Domain name" field, type the name of a Cisco EnergyWise domain where the Branch Circuit Monitor belongs. The domain name comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
4. In the "Domain password" field, type the authentication password (secret) for entering the Cisco EnergyWise domain. The password comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
5. In the Port field, type a User Datagram Protocol (UDP) port number for communication in the Cisco EnergyWise domain. The port ranges from 1 to 65535. Default is 43440.
6. In the "Polling interval" field, type a polling interval to determine how often the Branch Circuit Monitor is queried in the Cisco EnergyWise domain. The polling interval ranges from 30 to 600 seconds. Default is 180 seconds.
7. Click OK to save the changes.

Rebooting the Branch Circuit Monitor Device

You can remotely reboot the Branch Circuit Monitor device via the web interface.

To restart the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reboot the Branch Circuit Monitor.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the Branch Circuit Monitor device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

Channel Management

You can name each channel, including the mains and branch circuit channels, or monitor their status remotely.

Configuring the Mains Channels

To configure the mains channels, you must know the specifications of the CTs snapped onto the mains circuits. For information on the specifications of Raritan CTs, see ***CT Specifications*** (on page 298).

Warning: The information entered for the CT determines whether the Branch Circuit Monitor generates correct power measurements. Make sure you type or select the correct information. For any questions on the Raritan CT specifications, consult Raritan Technical Support.

To configure the mains channels:

1. Click the BCM folder.

Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Setup Circuits in the Settings section. The Circuit Setup dialog appears.
3. Select the Mains channel group and click Edit or simply double-click the channel group. The "Mains: L1, L2, L3 Configuration" dialog appears.
4. In the Transformer Type field, select the type of the mains CT you are using from the list. For Raritan mains CT, select Voltage.
5. In the Full-Scale Current (A) field, type the maximum current rating of your mains CT. For Raritan mains CT, type 200.
6. In the Full-Scale Voltage (mV) field, type the voltage supported by your mains CT. For Raritan mains CT, type 333.
7. Click OK in the configuration dialog to retain the changes.
8. Click OK to save the changes.

Important: The final step is required or the channel configuration changes are not saved.

Configuring the Branch Circuit Channels

To configure the branch circuit channels, you must know the specifications of the CTs snapped onto the branch circuits and whether the monitored branch circuit is single-phase or 3-phase. For information on the specifications of Raritan CTs, see ***CT Specifications*** (on page 298).

Warning: The information entered for the CT determines whether the Branch Circuit Monitor generates correct power measurements. Make sure you type or select the correct information. For any questions on the Raritan CT specifications, consult Raritan Technical Support.

To configure the branch circuit channels:

1. Click the BCM folder.

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Setup Circuits in the Settings section. The Circuit Setup dialog appears.
3. The branch circuit channels in this dialog are divided into various channel groups, each of which comprises 3 consecutive channels. Select the desired channel group and click Edit, or simply double-click the desired group. The "Branch Circuit: n1, n2, n3 Configuration" dialog appears (where n1, n2 and n3 are physical channel numbers).
4. In the Transformer Type field, select the type of the branch circuit CT you are using from the list. For Raritan branch circuit CTs, select Turns Ratio.

5. In the Turns Ratio field, type the turns ratio of the CTs connected to the selected channel group. For Raritan branch circuit CTs, type 2000 because its turns ratio is 1:2000.
6. In the Burden Resistor (Ohm) field, type the value of the burden resistor that is soldered into the Branch Circuit Monitor's board. Type 10 and never change it.
7. Specify the type of circuit (line) monitored by each channel group. There are two ways to set the circuit types:
   - If a group of channels is monitoring three single-phase branch circuits, do the following to make the three channels look as three "separate" single-phase channels in the tree:
     - Make sure the 3-Phase Wiring checkbox is deselected.
     - Select the appropriate circuit type (L1, L2 or L3) in the Phase A Connection field. The Phase A refers to the black channel. See ***Channel Convention*** (on page 6).
     - Select the appropriate circuit type (L1, L2 or L3) in the Phase B Connection field. The Phase B refers to the red channel.
     - Select the appropriate circuit type (L1, L2 or L3) in the Phase C Connection field. The Phase C refers to the blue channel.
     - If any channel is not connected to a CT or the CT connected to it is not snapped onto any conductor, select Unconnected instead.
   - If a group of channels is monitoring a 3-phase branch circuit, do the following to make the three channels look as "one" 3-phase channel in the tree:
     - Select the 3-Phase Wiring checkbox. The Phase A, B and C fields are automatically set to L1, L2 and L3 respectively.

     A 3-phase channel can provide the unbalance load status of the 3-phase branch circuit.
8. Click OK in the configuration dialog to retain the changes.
9. To configure additional branch circuit channels, repeat Steps 3 to 7.
10. Click OK to save the changes.

Important: The final step is required or the channel configuration changes are not saved.

Naming the Mains Channels

You can customize the mains' name for your own purpose. The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the character used to identify the mains, that is, M.

To name the Mains:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.
3. Click Setup. The Mains M Setup dialog appears.
4. Type a new name in the Name field.
5. Click OK to save the changes.

Naming Branch Circuit Channels

You can name each branch circuit channel for easily identifying them.

The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the physical channel number(s) associated with a branch circuit channel. For a single-phase branch circuit channel, the label is a channel number, such as 1, 2, 3 and so on. For a 3-phase branch circuit channel, the label consists of 3 channel numbers, such as 1-3, 4-6, 7-9 and so on. See **Configuring the Branch Circuit Channels** *(on page 77).*

To name a branch circuit channel:

1. Expand the Branch Circuits folder to show all branch circuit channels in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 49).
2. Click the desired branch circuit channel in the Dominion PX Explorer pane, and the page for this branch circuit channel opens in the right pane.
3. Click Setup. The Branch Circuit N Setup dialog appears, where N is a channel number or a range of channel numbers.

Tip: This dialog can be also triggered by clicking Setup on the Branch Circuits page when the Branch Circuits folder is selected in the Dominion PX Explorer pane.

4. Type a new name in the Name field.
5. Click OK to save the changes.

Monitoring the Mains Channels

You can view the mains' details, including its:

- Label (M)
- Customized name
- Mains sensor readings:
  - RMS current per line (A)
  - RMS voltage per line pair (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** *(on page 54).*

There are two ways to access the mains information.

To get the overview of the mains status:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Mains section on the Dashboard page.

To view the mains' details:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.

Monitoring the Branch Circuit Channels

The Dominion PX Explorer pane provides quick access to the branch circuit information. The branch circuit information, such as RMS current, active power, power factor, and so on, is displayed immediately after a branch circuit channel's icon is selected in the tree.

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

Monitoring All Channels

You can view the current status of all branch circuit channels at a time.

To monitor all channels:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click the Branch Circuits folder, and the Branch Circuits page opens in the right pane, showing all branch circuit channels with the following information:
   - Index number (#)
   - Channel name
   - Physical channel numbers in parentheses
   - Channel's sensor readings:
     - RMS current (A)
     - Active power (W)
     - Power factor

Tip: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** *(on page 54).*

Monitoring a Channel

To view a particular branch circuit channel's detailed information, follow this procedure.

To monitor a channel:

1. If the Branch Circuits folder is not expanded, expand it to show all branch circuit channels. See ***Expanding the Tree*** (on page 49).
2. Click the branch circuit channel you want in the Dominion PX Explorer pane, and the channel's details are shown in the right pane, including:
   - Label (that is, channel number)
   - Channel name
   - Line(s) associated with this channel
   - Channel's sensor readings:
     - RMS current (A)
     - RMS voltage (V)
     - Active power (W)
     - Apparent power (VA)
     - Power factor
     - Active energy (Wh)
     - Unbalanced load percentage (for a 3-phase branch circuit only)

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** *(on page 54).*

Setting Power Thresholds

Setting and enabling the thresholds causes the Branch Circuit Monitor to generate alert notifications when it detects that any component's power state crosses the thresholds.

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning range before the critical threshold.
- Upper and Lower Critical thresholds indicate the sensor reading is at the critical level.

To avoid generating a large amount of alert events, the deassertion hysteresis for each threshold is enabled. You can change the default hysteresis value if necessary. For more information on the deassertion hysteresis, see ***What is Deassertion Hysteresis?*** (on page 86).

Note: After setting the thresholds, remember to configure the event rules. See **Configuring Event Rules** *(on page 118).*

Setting the Mains Thresholds

You can set the mains thresholds so that the alerts are generated when the mains current and/or voltage crosses the thresholds.

To set the mains thresholds:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.
3. Click Setup. The Mains M Setup dialog appears.
4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.

   Tip: You can also double-click the desired sensor in the Threshold Configuration table to trigger this dialog.

6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.

- After any threshold is enabled, type an appropriate numeric value in the accompanying text box.

7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 86).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 88).
9. Click OK in the threshold setup dialog to retain the changes.
10. To set the thresholds for additional sensors, repeat Steps 4 to 9.
11. Click OK to save the changes.

Important: The final step is required or the threshold changes are not saved.

Setting the Branch Circuit Thresholds

You can set up the thresholds, deassertion hysteresis and assertion timeout for a particular branch circuit channel.

The threshold values set for an individual branch circuit channel will override the bulk threshold values stored on that channel.

Tip: To set up the thresholds, deassertion hysteresis and assertion timeout for multiple branch circuit channels at a time, see **Bulk Configuration for Branch Circuit Thresholds** *(on page 85).*

To set the thresholds for a branch circuit channel:

1. If the Branch Circuits folder is not expanded, expand it to show all branch circuit channels. See ***Expanding the Tree*** (on page 49).
2. Click the desired branch circuit channel in the Dominion PX Explorer pane, and the page for this branch circuit channel opens in the right pane.
3. Click Setup. The Branch Circuit N Setup dialog appears, where N is a channel number or a range of channel numbers.

   Tip: This dialog can be also triggered by clicking Setup on the Branch Circuits page when the Branch Circuits folder is selected in the Dominion PX Explorer pane.

4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.

   Tip: You can also double-click the desired sensor in the Threshold Configuration table to trigger this dialog.

6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 86).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 88).
9. Click OK in the threshold setup dialog to retain the changes.
10. To set the thresholds for additional sensors, repeat Steps 4 to 9.
11. Click OK to save the changes.

Important: The final step is required or the threshold changes are not saved.

Bulk Configuration for Branch Circuit Thresholds

The Branch Circuit Monitor allows you to set the power thresholds for multiple branch circuits at a time so that you can save time when configuring a number of branch circuit thresholds.

Note: To set the power thresholds for an individual branch circuit channel, you can either follow the instructions below or those described in the section **Setting the Branch Circuit Thresholds** *(on page 84).*

To configure thresholds, deassertion hysteresis and assertion timeout for multiple channels:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

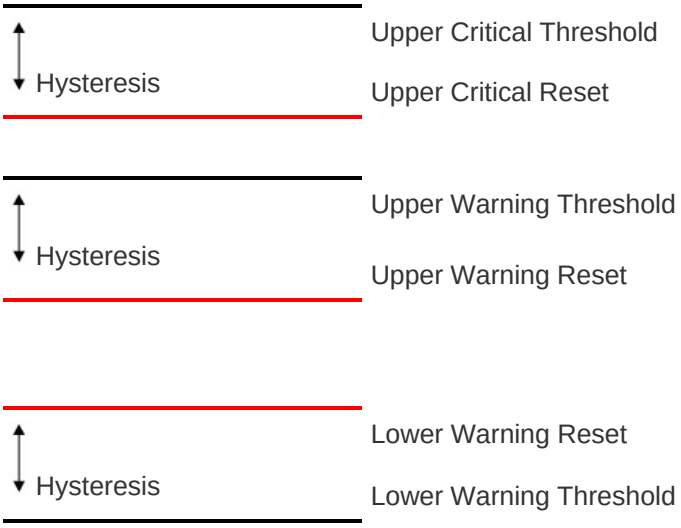
   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*
2. Click the Branch Circuits folder. The Branch Circuits page opens.
3. Click Bulk Setup. The Branch Circuit Threshold Bulk Setup dialog appears, with a list of all branch circuit channels.
4. In the Show Outlet Sensors of Type field, select the type of power thresholds you want to configure.
5. Select desired branch circuit channels by having their corresponding checkboxes selected.

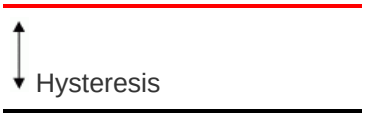
- To select all channels, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.
- To select partial channels, select the corresponding checkboxes of those channels by clicking on their checkboxes.
- To deselect any channel, just click on the checkbox once again.

6. Click Edit Thresholds. The threshold bulk setup dialog appears.
7. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
8. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 86).
9. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 88).
10. Click OK to save the changes.

What is Deassertion Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:





The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

Example: When Hysteresis is Useful

This example demonstrates when a deassertion hysteresis is useful.

The current critical threshold for L1 is set to 10 amps (A). The current draw rises to 11A, triggering a Current Critical alert. The current then continues to fluctuate between 9.1A and 11A.

With the hysteresis set to 1A, the Branch Circuit Monitor continues to indicate that the current on the branch circuit L1 is above critical. Without the hysteresis (that is, the hysteresis is set to zero), the Branch Circuit Monitor would de-assert the condition each time the current dropped to 9.9A, and re-assert the condition each time the current reached 10A or higher. With the fluctuating current, this could result in a number of repeating SNMP traps, and/or an e-mail account full of repeating SMTP alert notifications.

Example: When to Disable Hysteresis

This is an example of when you want to disable the hysteresis for a branch circuit #1. Hysteresis is disabled when its value is set to zero.

The upper warning threshold for current in the branch circuit #1 is set to 8A. In normal usage, the branch circuit #1 draws 7.6A of current. A spike in demand causes the current to reach 9A, triggering an alert. The current then settles to the normal draw of 7.6A.

With the hysteresis disabled, the Branch Circuit Monitor de-asserts the condition once the current drops to 7.9A. If the hysteresis is enabled and set to 1A, the branch circuit #1 would still be considered above the warning threshold as long as the current never dropped to 7A . The condition would not de-assert, even if the current returns to normal.

What is Assertion Timeout?

When the assertion timeout is enabled, the Branch Circuit Monitor device asserts any warning or critical condition only after a specified number of consecutive samples that cross a particular threshold are generated. This prevents a number of threshold alerts from being generated if the measurements return to normal immediately after rising above any upper threshold or dropping below any lower threshold.

User Management

The Branch Circuit Monitor is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full system permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's system permissions. See ***Setting Up Roles*** (on page 93).

Tip: By default, multiple users can log in simultaneously using the same login name.

Creating a User Profile

Creating new users adds a new login to the Branch Circuit Monitor.

To create a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Click New. The Create New User dialog appears.
3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to the Branch Circuit Monitor. ▪ The name can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are NOT permitted
Full Name	The user's first and last names.
Password,	The password the user enters to log in. Type it first

Field	Type this...
Confirm Password	in the Password field and then again in the Confirm Password field. ▪ The password can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are permitted.
Telephone Number	A phone number where the user can be reached.
eMail Address	An email address where the user can be reached. ▪ The email can be up to 32 characters long. ▪ It is case sensitive.

4. Select the Enabled checkbox. If not, the user CANNOT log in to the Branch Circuit Monitor device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.
6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring the SNMP Settings** *(on page 68).*

---

   b. Set up SNMPv3 parameters if enabling the SNMPv3 access permission.

Field	Description
Security Level	Click the drop-down arrow to select a preferred security level from the list: ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase,

Field	Description
	disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Authentication Pass Phrase	Re-type the same authentication pass phrase for confirmation.
Use Authentication Pass Phrase as Privacy Pass Phrase	*This checkbox is configurable only if AuthPriv is selected.* When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: ▪ DES (default) ▪ AES-128

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See ***Changing the SSH Settings*** (on page 67).
   a. Open the SSH public key with a text editor.
   b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.
8. Click the Roles tab to determine the permissions of the user.

9. Select one or multiple roles by selecting corresponding checkboxes.
   - The Admin role provides full permissions.
   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 93) for the scope of permissions. This role is selected by default.
   - If no roles meet your needs, you can:
     - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 94).
     - *Create a new role by clicking the Manage Roles button:* See ***Creating a Role*** (on page 93).

   Note: With multiple roles selected, a user has the union of all roles' permissions.

10. To change any measurement units displayed in the web interface for this new user, click the Preferences tab, and do any of the following:
    - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
    - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
    - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

    A Pascal is equal to one newton per square meter. Psi stands for pounds per square inch.

    Note: The measurement unit change only applies to the web interface and command line interface.

11. Click OK to save the changes.

Modifying a User Profile

You can change any user profile's information except for the user name.

To modify a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Make all necessary changes to the information shown.

To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.

5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 88).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 94).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

   Note: The measurement unit change only applies to the web interface and command line interface.
8. Click OK to save the changes.

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the User List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 55).

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

The Branch Circuit Monitor is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:

  - View Event Settings
  - View Local Event Log
  - Change Event Settings
  - Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
  - Change Own Password

  The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 88).

Creating a Role

Create a new role when you need a new combination of permissions.

To create a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.

6. Click OK to save the changes.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 88) or ***Modifying a User Profile*** (on page 91).

Modifying a Role

You can change an existing role's settings except for the name.

To modify a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to modify by clicking it.
3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

   Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.

4. Modify the text shown in the Description field if necessary.
5. To change the permissions, click the Privileges tab.

   Note: You cannot change the Admin role's permissions.

6. To delete any permissions, do this:
   a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   b. Click Delete.
7. To add any permissions, do this:
   a. Click Add. The Add Privileges to Role 'XXX' dialog appears, where XXX is the role name.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.
8. To change a specific permission's arguments, do this:
   a. Select the permission by clicking it.

b. Click Edit. The "Edit arguments of privilege 'XXX'" dialog appears, where XXX is the privilege name.

Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

c. Select the argument you want. You can make multiple selections.

d. Click OK.

9. Click OK to save the changes.

Deleting a Role

You can delete any role other than the Admin role.

To delete a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the Role List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 55).

Access Security Control

The Branch Circuit Monitor provides tools to control access. You can require HTTPS encryption, enable the internal firewall and create firewall rules, and create login limitations.

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up an SSL Certificate** *(on page 107) and* **Setting Up LDAP Authentication** *(on page 112).*

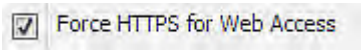
Forcing HTTPS Encryption

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the Branch Circuit Monitor device so it is a more secure protocol than HTTP.

You can force users to access the Branch Circuit Monitor web interface through the HTTPS protocol only. By default, this protocol is enabled.

To force HTTPS access to the web interface:

1. Choose Device Settings > Security > Force HTTPS for Web Access.
2. A message appears, prompting you to confirm the operation. Click Yes to enforce the HTTPS service.
3. Choose Device Settings > Security to verify the "Force HTTPS for Web Access" checkbox is selected as shown in this diagram.



If the checkbox is not selected, repeat these steps.

After enabling the HTTPS protocol, all access attempts using HTTP are redirected to HTTPS automatically.

Configuring the Firewall

The Branch Circuit Monitor has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the Branch Circuit Monitor device. By default the firewall is disabled.

To configure the firewall:

1. Enable the firewall. See ***Enabling the Firewall*** (on page 97).
2. Set the default policy. See ***Changing the Default Policy*** (on page 97).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 98).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device.

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

To enable the Branch Circuit Monitor firewall:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Select the Enable IP Access Control checkbox. This enables the firewall.
3. Click OK to save the changes.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access the Branch Circuit Monitor.

You can change the default policy to Drop or Reject, in which case traffic from all IP addresses is discarded except the IP addresses accepted by a specific rule.

To change the default policy:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
   - Accept: Accepts traffic from all IP addresses.
   - Drop: Discards traffic from all IP addresses, without sending any failure notification to the source host.
   - Reject: Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.
4. Click OK to save the changes. The new default policy is applied.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic intended for the Branch Circuit Monitor, based on the IP address of the host sending the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches the Branch Circuit Monitor device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the Branch Circuit Monitor.

- **Subnet mask may be required.**

  When typing the IP address, you may or may not need to specify BOTH the address and a subnet mask. The default subnet mask is /32 (that is, 255.255.255.255). You must specify a subnet mask only when it is not the same as the default. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IP addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IP addresses entered are within the scope.

To create firewall rules:

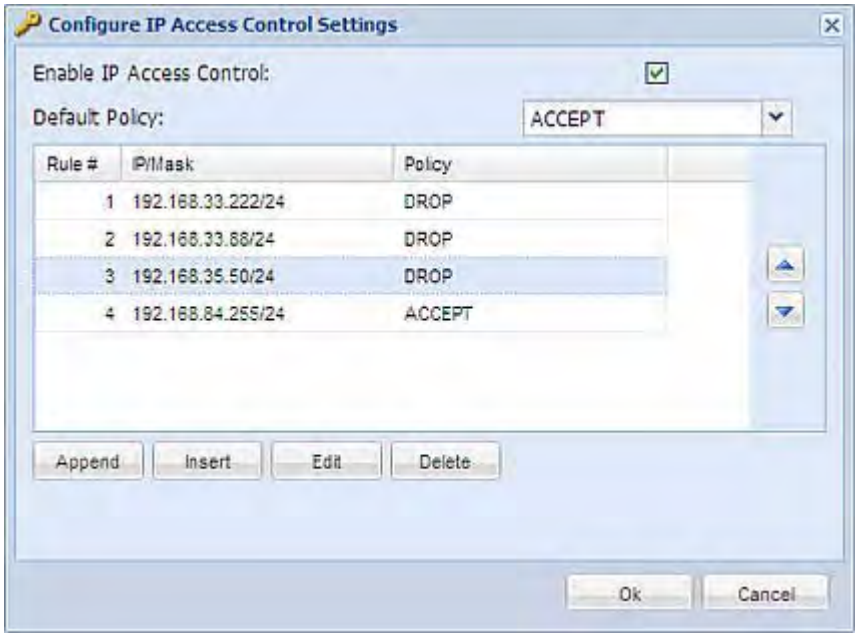
1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Create specific rules. See the table for different operations.

Action	Procedure

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

Action	Procedure
	▪ Click OK to save the changes. The system automatically numbers the rule.
Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. ▪ Accept: Accepts traffic from the specified IP address(es). ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host. ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification. ▪ Click OK to save the changes. The system inserts the rule and automatically renumbers the following rules.

4. When finished, the rules appear in the Configure IP Access Control Settings dialog.



5. Click OK to save the changes. The rules are applied.

Editing Firewall Rules

When an existing firewall rule requires updates of IP address range and/or policy, modify them accordingly.

To modify a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select the rule to be modified in the rules list.
4. Click Edit or double-click the rule. The Edit Rule dialog appears.
5. Make changes to the information shown.
6. Click OK to save the changes.
7. Click OK to quit the Configure IP Access Control Settings dialog, or the changes are lost.

Sorting Firewall Rules

The rule order determines which one of the rules matching the same IP address is performed.

To sort the firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select a specific rule by clicking it.
4. Click or to move the selected rule up or down until it reaches the desired location.
5. Click OK to save the changes.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Ensure the Enable IP Access Control checkbox is selected.
3. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

4. Click Delete.
5. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
6. Click OK to save the changes.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the Branch Circuit Monitor and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to the Branch Circuit Monitor and fail authentication before the user's login is blocked.

Note that this function applies only to local authentication instead of authentication through external AA servers.

Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a serial connection. See **Unblocking a User** *(on page 291).*

To enable user blocking:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.
3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user's login is blocked from accessing the Branch Circuit Monitor device.
5. To determine how long the login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
   - Infinite: This option sets no time limit on blocking the login.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.

6. Click OK to save the changes.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and how long users are permitted to stay idle before being forced to log out.

To enable login limitations:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the Login Limitations section.
3. To prevent more than one person from using the same login at the same time, select the "Prevent concurrent login with same username" checkbox.
4. To adjust how long users can remain idle before they are forcibly logged out by the Branch Circuit Monitor, select a time option in the Idle Timeout Period field. The default is 10 minutes.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

   Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.
5. Click OK to save the changes.

Tip: Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the Branch Circuit Monitor.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the Branch Circuit Monitor device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

To force users to create strong passwords:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of restricted passwords in history	= 5

Note: The maximum password length accepted by the Branch Circuit Monitor is 32 characters.

3. Make necessary changes to the default settings.
4. Click OK to save the changes.

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default interval is 60 days.

To force users to change passwords regularly:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Password Aging checkbox to enable the password aging feature.
3. To determine how often users are requested to change their passwords, select a number of days in the Password Aging Interval field. Users are required to change their password every time that number of days has passed.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "9 d" to set the password aging time to 9 days.

4. Click OK to save the changes.

Setting Up Role-Based Access Control Rules

Role-based access control rules are similar to firewall rules, except they are applied to members sharing a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

To set up role-based access control rules:

1. Enable the feature. See ***Enabling the Feature*** (on page 104).
2. Set the default policy. See ***Changing the Default Policy*** (on page 104).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role-Based Access Control Rules*** (on page 105).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

To enable role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Select the Enable Role Based Access Control checkbox. This enables the feature.
3. Click OK to save the changes.

Changing the Default Policy

The default policy is to accept all traffic from all IP addresses regardless of the role applied to the user.

To change the default policy:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Make sure the Enable Role Based Access Control checkbox is selected.
3. Select the action you want from the Default Policy drop-down list.

- Allow: Accepts traffic from all IP addresses regardless of the user's role.
- Deny: Drops traffic from all IP addresses regardless of the user's role.

4. Click OK to save the changes.

Creating Role-Based Access Control Rules

Role-based access control rules accept or drop traffic, based on the user's role and IP address. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

To create role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Make sure the Enable Role Based Access Control checkbox is selected.
3. Create specific rules:

Action	Do this...

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type a starting IP address in the Starting IP Address field.
	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK to save the changes.
	The system automatically numbers the rule.

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address

Action	Do this...
	field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role ▪ Click OK to save the changes. The system inserts the rule and automatically renumbers the following rules.

4. Click OK to save the changes.

Editing Role-Based Access Control Rules

You can modify existing rules when these rules do not meet your needs.

To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select the rule to be modified in the rules list.
4. Click Edit or double-click the rule. The Edit Rule dialog appears.
5. Make changes to the information shown.
6. Click OK to save the changes.

Sorting Role-Based Access Control Rules

Similar to firewall rules, the order of role-based access control rules determines which one of the rules matching the same IP address is performed.

To sort role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.

2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select a specific rule by clicking it.
4. Click or to move the selected rule up or down until it reaches the desired location.
5. Click OK to save the changes.

Deleting Role-Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

To delete a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Ensure the Enabled Role Based Access Control checkbox is selected.
3. Select the rule to be deleted in the rules list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
4. Click Delete.
5. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
6. Click OK to save the changes.

Setting Up an SSL Certificate

Having an X.509 digital certificate ensures that both parties in an SSL connection are who they say they are.

To obtain a certificate for the Branch Circuit Monitor, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with an SSL certificate, which you must install on the Branch Circuit Monitor device.

Note: See **Forcing HTTPS Encryption** *(on page 96) for instructions on forcing users to employ SSL when connecting to the Branch Circuit Monitor.*

A CSR is not required in either of the following scenarios:

- You decide to generate a *self-signed* certificate on the Branch Circuit Monitor device.
- Appropriate, valid certificate and key files have been available.

Certificate Signing Request

When appropriate certificate and key files for the Branch Circuit Monitor are NOT available, one of the alternatives is to create a CSR and private key on the Branch Circuit Monitor device, and send the CSR to a CA for signing the certificate.

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your Branch Circuit Monitor device.

To create a CSR:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.
   - In the Subject section:

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Branch Circuit Monitor device.
Email Address	An email address where you or another administrative user can be reached.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields. If you generate a CSR without values entered in the required fields, you cannot obtain third party certificates.

   - In the Key Creation Parameters section:

Field	Do this
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the Branch Circuit Monitor device's response.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional, and the value should be 4 to 64 characters long. The password is case sensitive, so ensure you capitalize the letters correctly.
Confirm Challenge	Type the same password again for confirmation.

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
   a. You are prompted to open or save the file. Click Save to save it on your computer.
   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
   c. If desired, click Delete Certificate Signing Request to remove the CSR file permanently from the Branch Circuit Monitor device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the Branch Circuit Monitor device.

To install the certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. In the Certificate File field, click Browse to select the certificate file provided by the CA.

4. Click Upload. The certificate is installed on the Branch Circuit Monitor device.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the Branch Circuit Monitor device are unavailable, the alternative other than submitting a CSR to the CA is to generate a self-signed certificate.

To create and install a self-signed certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your Branch Circuit Monitor device.
Email Address	An email address where you or another administrative user can be reached.
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the Branch Circuit Monitor device's response.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate is valid in this field.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear after the Self Sign checkbox is selected.

4. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.
5. You can also do any of the following:
   - Click "Install Key and Certificate" to immediately install the self-signed certificate and private key. When any confirmation and security messages appear, click Yes to continue.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

   - To download the self-signed certificate or private key, click Download Certificate or Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
   - To remove the self-signed certificate and private key permanently from the Branch Circuit Monitor device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the Branch Circuit Monitor device resets and the login page re-opens.

Installing Existing Key and Certificate Files

If the SSL certificate and private key files are already available, you can install them directly without going through the process of creating a CSR or a self-signed certificate.

To install the existing key and certificate files:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the Branch Circuit Monitor device.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.
7. Click Close to quit the dialog.

Downloading Key and Certificate Files

You can download the key and certificate files currently installed on the Branch Circuit Monitor device for backup or other operations. For example, you can install the files on a replacement Branch Circuit Monitor device, add the certificate to your browser and so on.

To download the certificate and key files from a Branch Circuit Monitor device:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. The Active SSL Certificate tab should open. If not, click it.
3. Click Download Key to download the private key file installed on the Branch Circuit Monitor device. You are prompted to open or save the file. Click Save to save it on your computer.
4. Click Download Certificate to download the certificate file installed on the Branch Circuit Monitor device. You are prompted to open or save the file. Click Save to save it on your computer.
5. Click Close to quit the dialog.

Setting Up LDAP Authentication

For security purposes, users attempting to log in to the Branch Circuit Monitor must be authenticated. The Branch Circuit Monitor supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the Branch Circuit Monitor device
- Lightweight Directory Access Protocol (LDAP)

By default, the Branch Circuit Monitor is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user. If you prefer to use an external LDAP server, you must:

- Provide the Branch Circuit Monitor with information about the LDAP server.
- Create user profiles for users who are authenticated externally because a user profile on the Branch Circuit Monitor device determines the role(s) applied to the user, and determines the permissions for the user accordingly.

When configured for LDAP authentication, all Branch Circuit Monitor users must have an account on the LDAP server. Local-authentication-only users will have no access to the Branch Circuit Monitor except for the admin, who always can access the Branch Circuit Monitor.

Gathering the LDAP Information

It requires knowledge of your LDAP server and directory settings to configure the Branch Circuit Monitor for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over SSL) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*
    - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Adding the LDAP Server Settings

To activate and use external LDAP/LDAPS server authentication, enable LDAP authentication and enter the information you have gathered for any LDAP/LDAPS server.

Note: An LDAPS server refers to an SSL-secured LDAP server.

To add the LDAP/LDAPS server settings:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.

4. IP Address / Hostname - Type the IP address or hostname of your LDAP/LDAPS authentication server.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

5. Type of external LDAP/LDAPS server. Choose from among the options available:
   - OpenLDAP
   - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
6. LDAP over SSL - Select this checkbox if you would like to use SSL. Secure Sockets Layer (SSL) is a cryptographic protocol that allows the Branch Circuit Monitor to communicate securely with the LDAP/LDAPS server. A certificate file is required when enabling the encryption.
7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the "LDAP over SSL" checkbox is selected.
9. Use only trusted LDAP Server Certificates - Select this checkbox if you would like to use a trusted LDAP server certificate file, that is, a certificate file signed by the CA. When NOT selected, you can use all LDAP/LDAPS server certificates, including a self-signed certificate file.
10. Server Certificate - Consult your authentication server administrator to get the CA certificate file for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is required when the "LDAP over SSL" checkbox is selected.
11. Anonymous Bind - For "OpenLDAP," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, select this checkbox.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
12. Use Bind Credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, deselect this checkbox. By default it is deselected.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.

13. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base. This information is required only when the Use Bind Credentials checkbox is selected.
14. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required only when the Use Bind Credentials checkbox is selected.
15. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
16. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
    - Login name attribute (also called AuthorizationString)
    - User entry object class
    - User search subfilter (also called BaseSearch)

    Note: The Branch Circuit Monitor will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.
17. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
18. To verify if the LDAP/LDAPS configuration is done correctly, you may click Test Connection to check whether the Branch Circuit Monitor can connect to the LDAP/LDAPS server successfully.

    Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.
19. Click OK to save the changes. The new LDAP server is listed in the Authentication Settings dialog.
20. To add additional LDAP/LDAPS servers, repeat Steps 3 to 19.
21. Click OK to save the changes. The LDAP authentication is now in place.

Note: If the Branch Circuit Monitor clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the Branch Circuit Monitor and the LDAP server to use the same NTP server.

More Information about AD Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 306).

Sorting the LDAP Access Order

The order of the LDAP list determines the access priority of remote LDAP/LDAPS servers. The Branch Circuit Monitor first tries to access the top LDAP/LDAPS server in the list for authentication, then the next one if the access to the first one fails, and so on until the Branch Circuit Monitor device successfully connects to one of the listed LDAP/LDAPS servers.

Note: After successfully connecting to one LDAP/LDAPS server, the Branch Circuit Monitor STOPS trying to access the remaining LDAP/LDAPS servers in the list regardless of the user authentication result.

To re-sort the LDAP server access list:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server whose priority you want to change.
3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK to save the changes.

Testing the LDAP Server Connection

You can test the connection to any LDAP/LDAPS server to verify the server accessibility or the validity of the authentication settings.

To test the connection to an LDAP/LDAPS server:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to test.
3. Click Test Connection to start the connection test.

Editing the LDAP Server Settings

If the configuration on any LDAP/LDAPS server has been changed, such as the port number, bind DN and password, you must modify the LDAP/LDAPS settings on the Branch Circuit Monitor device accordingly, or the authentication fails.

To modify the LDAP authentication configuration:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to edit.
3. Click Edit. The Edit LDAP Server Configuration dialog appears.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

Deleting the LDAP Server Settings

You can delete the authentication settings of a specific LDAP/LDAPS server when the server is not available or used for remote authentication.

To remove one or multiple LDAP/LDAPS servers:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK to save the changes.

Disabling the LDAP Authentication

When the remote authentication service is disabled, the Branch Circuit Monitor authenticates users against the local database stored on the Branch Circuit Monitor device.

To disable the LDAP authentication service:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Local Authentication radio button.
3. Click OK to save the changes.

Enabling LDAP and Local Authentication Services

To make authentication function properly all the time -- even when external authentication is not available, you can enable both the local and remote authentication services.

When both authentication services are enabled, the Branch Circuit Monitor follows these rules for authentication:

- When any of the LDAP/LDAPS servers in the access list is accessible, the Branch Circuit Monitor authenticates against the connected LDAP/LDAPS server only.
- When the connection to every LDAP/LDAPS server fails, the Branch Circuit Monitor allows authentication against the local database.

To enable both authentication services:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Ensure the LDAP radio button has been selected.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK to save the changes.

Configuring Event Rules

A benefit of the product's intelligence is its ability to notify you of and react to a change in conditions. This event notification or reaction is an "event rule."

The Branch Circuit Monitor is shipped with two built-in event rules, which cannot be deleted.

- System Event Log Rule: This rule causes ANY event occurred to the Branch Circuit Monitor to be recorded in the internal log. The rule is enabled by default.
- System SNMP Trap Rule: This rule causes SNMP traps to be sent to specified IP addresses or hosts when ANY event occurs to the Branch Circuit Monitor. The rule is disabled by default.

If these two do not satisfy your needs, you can create additional rules to respond to different events.

Note: Internet Explorer® 8 (IE8) does not use compiled JAVA script. When using IE8 to create or change event rules, the CPU performance may be degraded, resulting in the appearance of the connection time out message. When this occurs, click Ignore to continue.

Components of an Event Rule

An event rule defines what the Branch Circuit Monitor does in certain situations and is composed of two parts:

- Event: This is the situation where the Branch Circuit Monitor or part of it meets a certain condition. For example, the inlet's voltage exceeds the warning threshold.
- Action: This is the response to the event. For example, the Branch Circuit Monitor notifies the system administrator of the event and records the event in the log.

Creating an Event Rule

The best way to create a new set of event rule, in sequence, is:

- Create actions for responding to one or multiple events.
- Create rules to determine what actions are taken when these events occur.

Creating Actions

The Branch Circuit Monitor comes with two built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Trap Action: This action sends SNMP traps to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for the "System SNMP Trap Action" by default so you must specify IP addresses before applying this action to any event rule.

The built-in actions cannot be deleted. If these actions do not satisfy your needs, then create new ones.

To create new actions:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New Action.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number.
5. In the Action field, click the drop-down arrow, and select the desired action from the list in response to the selected event.

Option	Description
Log event message	This option records the selected events in the internal log.
Send Image via SMTP	This option notifies one or multiple persons of the selected events by emailing the images captured by a connected Logitech® QuickCam® Pro 9000 Webcam (if any). ▪ In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses. ▪ To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 74) for the information of each field.
Send SMTP message	This option notifies one or multiple persons of the selected events by e-mail. ▪ In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses. ▪ To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 74) for the information of each field.

Option	Description
Send SNMP trap	This option sends SNMP traps to one or multiple SNMP managers. ▪ You can specify up to 3 SNMP trap destinations in the Host *x* fields, where *x* is a number between 1 and 3. ▪ Specify a port number for each destination in the Port *x* fields, where *x* is a number between 1 and 3. ▪ Specify a community string for each destination in the Community *x* fields, where *x* is a number between 1 and 3.
Syslog message	This option makes the Branch Circuit Monitor automatically forward event messages to the specified syslog server. ▪ In the "Syslog server" field, specify the IP address to which syslog is forwarded. ▪ In the Port field, specify an appropriate port number.

6. Click Save to save the new action.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

7. To create additional actions, repeat Steps 3 to 7.
8. Click Close to quit the dialog.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, the Branch Circuit Monitor provides two built-in event rules -- System Event Log Rule and System SNMP Trap Rule. If the built-in rules do not satisfy you needs, create new ones.

Note: For information on the built-in event rules, see **Configuring Event Rules** *(on page 118).*

To create event rules:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, click New Rule.

3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enabled checkbox to enable this event rule.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing all types of events appears.
   - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

Note: The option <Any sub-event> refers to all events/items listed on the same submenu, <Any slot> refers to all slots, <Any server> refers to all servers, and <Any user> refers to all users. <Any Branch> refers to all branch circuit channels.

6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or asset tag connections or disconnections	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The Branch Circuit Monitor takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The Branch Circuit Monitor takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The Branch Circuit Monitor takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts).
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed," "No longer alarmed" and "Both." ▪ Alarmed: The Branch Circuit Monitor takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The Branch Circuit Monitor takes the action only when the chosen sensor returns to normal. ▪ Both: The Branch Circuit Monitor takes the action both when the chosen sensor enters or quits the alarmed state.

Event types	Radio buttons
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The Branch Circuit Monitor takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The Branch Circuit Monitor takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The Branch Circuit Monitor takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	Available radio buttons include "Link state is up," "Link state is down" and "Both." ▪ Link state is up: The Branch Circuit Monitor takes the action only when the network link state changes from down to up. ▪ Link state is down: The Branch Circuit Monitor takes the action only when the network link state changes from up to down. ▪ Both: The Branch Circuit Monitor takes the action whenever the network link state changes.
Function enabled or disabled	Available radio buttons include "Enabled," "Disabled" and "Both." ▪ Enabled: The Branch Circuit Monitor takes the action only when the chosen function is enabled. ▪ Disabled: The Branch Circuit Monitor takes the action only when the chosen function is disabled. ▪ Both: The Branch Circuit Monitor takes the action when the chosen function is either enabled or disabled.
User login or logout	Available radio buttons include "Logged in," "Logged out," and "Both." ▪ Logged in: The Branch Circuit Monitor takes the action only when the selected user logs in. ▪ Logged out: The Branch Circuit Monitor takes the action only when the selected user logs out. ▪ Both: The Branch Circuit Monitor takes the action both when the selected user logs in and logs out.

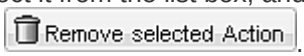
Event types	Radio buttons
Server monitoring event	Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both." ▪ Monitoring started: The Branch Circuit Monitor takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The Branch Circuit Monitor takes the action only when the monitoring of any specified server stops. ▪ Both: The Branch Circuit Monitor takes the action when the monitoring of any specified server starts or stops.
Server reachability	Available radio buttons include "Unreachable," "Reachable," and "Both." ▪ Unreachable: The Branch Circuit Monitor takes the action only when any specified server becomes inaccessible. ▪ Reachable: The Branch Circuit Monitor takes the action only when any specified server becomes accessible. ▪ Both: The Branch Circuit Monitor takes the action when any specified server becomes either inaccessible or accessible.
RF Code tag connection or disconnection	Available radio buttons include "Connected," "Disconnected" and "Both." ▪ Connected: Branch Circuit Monitor takes the action only when an RF Code tag is physically connected to it. ▪ Disconnected: Branch Circuit Monitor takes the action only when an RF Code tag is physically disconnected from it. ▪ Both: Branch Circuit Monitor takes the action both when the RF Code tag is physically connected to it and when it is disconnected.

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

7. In the Actions field, click the drop-down arrow, select the desired action from the list, and click the Add Action button

to add the action.

   The added action will be listed in the list box to the right of the Actions filed.

8. To add additional actions, repeat Step 7.
9. To remove any added action, select it from the list box, and click the "Remove selected Action" button 

.
10. Click Save to save the new event rule.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

11. Repeat the same steps to create additional event rules.
12. Click Close to quit the dialog.

Sample Event Rules

Sample Device-Level Event Rule

In this example, we want the Branch Circuit Monitor to record the firmware upgrade failure in the internal log when it happens. The sample event rule looks like this:

- Event: Event > Device > Firmware update failed
- Actions: System Event Log Action

To create the above event rule:

1. Select Event > Device to indicate we are specifying an event at the device level.
2. Select "Firmware update failed" in the submenu because we want the Branch Circuit Monitor to respond to the event related to firmware upgrade failure.
3. Select System Event Log Action as we intend to record the firmware update failure event in the internal log.

Sample Mains-Level Event Rule

In this example, we want the Branch Circuit Monitor to send SNMP traps to the SNMP manager both when any Mains sensor reading crosses any threshold and when the reading becomes unavailable. The event rule is set like this:

- Event: Event > Mains > Mains M > Sensor > Any sub-event
- Actions: System SNMP Trap Action

To create the above event rule:

1. Select Event > Mains to indicate we are specifying an event at the mains level.
2. Select "Mains M" from the submenu because that is the target.

3. Select "Sensor" to refer to sensor readings.
4. Select "Any sub-event" because we want to specify all events related to all types of Mains sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Trap Action" to send SNMP traps to respond to the specified event.

Sample Branch Circuit-Level Event Rule

In this example, we want the Branch Circuit Monitor to send SNMP traps to the SNMP manager both when any sensor reading of branch circuit channel #3 crosses any threshold and when the sensor reading becomes unavailable. To do that we would set up an event rule like this:

- Event: Event > Branch Circuits > Branch 3 > Sensor > Any sub-event
- Actions: System SNMP Trap Action

To create the above event rule:

1. Select Event > Branch Circuits to indicate we are specifying an event at the branch circuit level.
2. Select "Branch 3" from the submenu because that is the branch circuit channel in question.
3. Select "Sensor" to refer to sensor readings.
4. Select "Any sub-event" because we want to specify all events related to all types of branch circuit sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Trap Action" to send SNMP traps to respond to the specified event.

Modifying an Event Rule

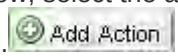
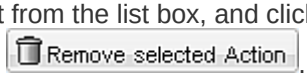
You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule and System SNMP Trap Rule.

To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify in the left pane.

3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

   For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all user names (referred to as <*Any user*>).
5. If radio buttons are available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
   - To add a new action, click the drop-down arrow, select the action from the list, and click the Add Action button . 
   - To remove any added action, select it from the list box, and click the "Remove selected Action" button  .
7. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.
8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in action "System Event Log Action" is not user-configurable.

To modify an action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify from the left list.
4. Make necessary changes to the information shown.
5. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.
6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

To delete an event rule or action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the left list, and click Delete Rule.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the left list, and click Delete Action.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the Branch Circuit Monitor to generate an alert. The measurement then returns to a value within the threshold, but the Branch Circuit Monitor does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the Branch Circuit Monitor uses. See ***What is Deassertion Hysteresis?*** (on page 86).

Managing Event Logging

By default, the Branch Circuit Monitor captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view up to 2,000 historical events that occurred to the Branch Circuit Monitor device in the local event log.

When the log already contains 2,000 entries, each new entry overwrites the oldest entry.

To display the local log:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

   Each event entry in the local log consists of:

   - Date and time of the event
   - Type of the event
   - A description of the event
   - ID number of the event

2. The dialog shows the final page by default. You can:

   - Switch between different pages by doing one of the following:

     - Click ⏮ or ⏭ to go to the first or final page.

     - Click ◀ or ▶ to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.

   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » and select Show Details to view details.

   - Click ⏭ to view the latest events.

3. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 57).
4. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 55).
5. Click Close to quit the dialog.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

To delete all event entries:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

2. Click Clear Event Log.
3. Click Close to quit the dialog.

Viewing Connected Users

You can see which users are being connected to the Branch Circuit Monitor device and their status in the web interface. Besides, if you have the administrator privileges, you can terminate any user's connection to the Branch Circuit Monitor device.

To view connected users:

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a serial connection, <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the Branch Circuit Monitor. ▪ Web GUI: Refers to the Branch Circuit Monitor web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user was connected to the CLI. - *Serial*: Represents the local connection (serial or USB). - *SSH*: Represents the SSH connection. - *Telnet*: Represents the Telnet connection.
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
   a. A dialog appears, prompting you to confirm the operation.
   b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out.
3. You may change the sorting order of the list if necessary. See ***Changing the Sorting*** (on page 56).
4. Click Close to quit the dialog.

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the Branch Circuit Monitor device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

Adding IT Devices for Ping Monitoring

You can have the Branch Circuit Monitor monitor the accessibility of any IT equipment, such as DB servers and remote authentication servers.

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable Ping Monitoring for this Server" checkbox is selected. If not, select it to enable the ping monitoring feature.
4. Provide the information required.

Field	Description
IP Address/Hostname	IP address or host name of the IT equipment whose accessibility you want to monitor.
Number of Successful Pings to Enable Feature	The number of successful pings required to enable this feature. Valid range is 0 to 200.
Wait Time (in seconds) after Successful Ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait Time (in seconds) after Unsuccessful Ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of Consecutive Unsuccessful Pings for Failure	The number of consecutive pings without any response before the IT equipment is declared unresponsive. Valid range is 1 to 100.
Wait Time (in seconds) before Resuming Pinging	The wait time before resuming pinging after the IT equipment is declared unresponsive. Valid range is 1 to 1200 (seconds).

5. Click OK to save the changes.
6. To add more IT devices, repeat Steps 2 to 5.

7. Click Close to quit the dialog.

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever it requires changes.

To modify the ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify by clicking it.
3. Click Edit or double-click the IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK to save the changes.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose ping monitoring settings you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying servers for the Branch Circuit Monitor device to monitor.

To check the server monitoring states and results:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding server is activated or not.

- : This icon denotes that the monitoring for the corresponding server is enabled.
- : This icon denotes that the monitoring for the corresponding server is disabled.

3. The column labeled "Status" indicates the accessibility of each monitored server.

Status	Description
Reachable	The server is accessible.
Unreachable	The server is inaccessible.
Waiting for reliable connection	The connection between the Branch Circuit Monitor device and the server is not established yet.

4. You may change the sorting order of the list if necessary. See ***Changing the Sorting*** (on page 56).
5. Click Close to quit the dialog.

Environmental Sensors

The Branch Circuit Monitor can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed.

To add environmental sensors:

1. Physically connect environmental sensors to the Branch Circuit Monitor device. See ***Connecting Environmental Sensors (Optional)*** (on page 26).
2. Log in to the Branch Circuit Monitor web interface. The Branch Circuit Monitor should have detected the connected sensors, and display them in the web interface.
3. Identify each sensor through the sensor's serial number. See ***Identifying Environmental Sensors*** (on page 134).
4. The Branch Circuit Monitor should automatically manage the detected sensors. Verify whether detected sensors are managed. If not, have them managed. See ***Managing Environmental Sensors*** (on page 135).
5. Configure the sensors. See ***Configuring Environmental Sensors*** (on page 136). The steps include:
   a. Name the sensor.
   b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
   c. Mark the sensor's physical location on the rack or in the room.

d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state. Only numeric sensors have the threshold settings.

Identifying Environmental Sensors

An environmental sensor includes a serial number tag on the sensor cable.

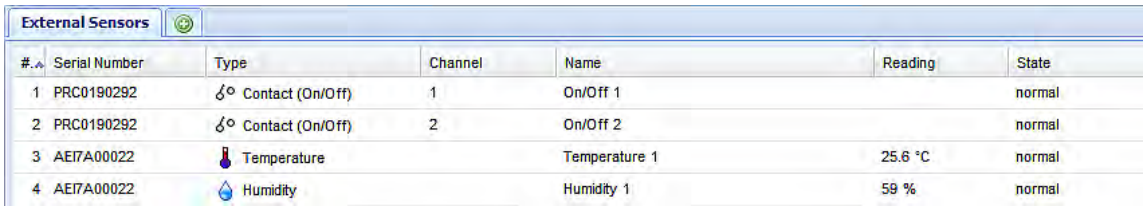
The serial number for each sensor appears listed in the web interface after each sensor is detected by the Branch Circuit Monitor.

To identify each detected environmental sensor:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.



#.	Serial Number	Type	Channel	Name	Reading	State
1	PRC0190292	Contact (On/Off)	1	On/Off 1		normal
2	PRC0190292	Contact (On/Off)	2	On/Off 2		normal
3	AEI7A00022	Temperature		Temperature 1	25.6 °C	normal
4	AEI7A00022	Humidity		Humidity 1	59 %	normal

3. Match the serial number from the tag to those listed in the sensor table.

Managing Environmental Sensors

The Branch Circuit Monitor starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed.

The Branch Circuit Monitor device can manage a maximum of 16 environmental sensors.

When there are less than 16 managed sensors, the Branch Circuit Monitor automatically brings detected environmental sensors under management. You should only have to manually manage a sensor when it is not under management.

To manually manage an environmental sensor:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to manage on the External Sensors page.

   Note: To identify all detected sensors, see **Identifying Environmental Sensors** *(on page 134).*

4. Click Manage. The "Manage sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor's serial number and <sensor type> is the sensor's type.

   Note: For a contact closure sensor, a channel number is added to the end of the <sensor type>.

5. There are two ways to manage the sensor:
   - To manage this sensor by letting the Branch Circuit Monitor assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors.
   - To manage this sensor by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

     If the number you selected was already assigned to a sensor, that sensor becomes released after losing this ID number.

   Tip: The information in parentheses following each ID number indicates whether the number has been assigned to any sensor. If it has been assigned to a sensor, it shows that sensor's serial number. Otherwise, it shows the term "unused."

6. Click OK. The Branch Circuit Monitor starts to track and display the managed sensor's reading and/or state.
7. To manage additional sensors, repeat Steps 3 to 6.

Note: When the number of managed sensors reaches the maximum, you CANNOT manage additional sensors until you remove or replace any managed sensors. To remove a sensor, see **Unmanaging Environmental Sensors** *(on page 142).*

Configuring Environmental Sensors

You may change the default name for easily identifying the managed sensor, and describe its location with X, Y and Z coordinates.

To configure environmental sensors:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the sensor that you want to configure.
4. Click Setup. The "Setup of external sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the serial number of this sensor and <sensor type> is the sensor's type.

   Tip: You can also trigger the same setup dialog by selecting the desired environmental sensor icon in the tree and then clicking Setup on that sensor's page opened in the right pane.

5. If the selected environmental sensor is the Raritan contact closure sensor connected with a third-party detector/switch, select the appropriate sensor type in the Binary Sensor Subtype field.
   - Contact: The detector/switch is designed to detect the door lock or door open/closed status.
   - Smoke Detection: The detector/switch is designed to detect the appearance of smoke.
   - Water Detection: The detector/switch is designed to detect the appearance of water on the floor.
   - Vibration: The detector/switch is designed to detect the vibration in the floor.
6. Type a new name in the Name field.

7. Describe the sensor's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor Location*** (on page 138).

   Note: When the term "Rack Units" appears inside the parentheses in the Z location field, indicating that the Z coordinate format is set to Rack Units, you must type an integer number.

8. If the selected environmental sensor is a numeric sensor, its threshold settings are displayed in the dialog. Click Edit or double-click the Threshold Configuration table to adjust the threshold, deassertion hysteresis and assertion timeout settings.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 86).
   - To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 88).

   Note: The Upper Critical and Lower Critical values are points at which the Branch Circuit Monitor considers the operating environment critical and outside the range of the acceptable threshold.

9. Click OK to save the changes.
10. Repeat the same steps to configure additional environmental sensors.

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors.

To determine the Z coordinate format:

1. Click the BCM folder.

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click Setup in the Settings section. The BCM Setup dialog appears.
3. In the "External sensors Z coordinate format" field, click the drop-down arrow and select an option from the list.

- Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
- Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.

4. Click OK to save the changes.

Describing the Sensor Location

Use the X, Y and Z coordinates to describe each sensor's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 32 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 32 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the Branch Circuit Monitor MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** *(on page 161).*

Viewing Sensor Data

Readings of the environmental sensors will display in the web interface after these sensors are properly connected and managed.

The Dashboard page shows the information for managed environmental sensors only, while the External Sensors page shows the information for both of managed and unmanaged ones.

If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See ***The Yellow- or Red-Highlighted Reading*** (on page 54).

To view managed environmental sensors only:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the External Sensors section on the Dashboard page. The section shows:
   - Total number of managed sensors
   - Total number of unmanaged sensors
   - Information of each managed sensor, including:
     - Name
     - Reading
     - State

To view both of managed and unmanaged environmental sensors:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.

   Detailed information for each connected sensor is displayed, including:
   - Label (number)
   - Serial number
   - Sensor type
   - Name
   - Reading

- State
- Channel (for a contact closure sensor only)

Sensor Measurement Accuracy

Raritan environmental sensors are with the following factory specifications. Calibration is not required for environmental sensors.

- Temperature: +/-2%
- Humidity: +/-5%
- Differential air pressure: +/-1.5%
- Air flow: +/-6.5%

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete. For example, a contact closure sensor is a discrete sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity to the sensor is lost.

The Branch Circuit Monitor pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor module show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The Branch Circuit Monitor continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

Note: See **Configuring a Contact Closure Sensor** *(on page 29) for setting the normal state.*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

Lower Warning threshold <= Reading < Upper Warning threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

For a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

Note: See **Configuring a Contact Closure Sensor** *(on page 29) for setting the normal state.*

Tip: A contact closure sensor's LED is lit after entering the alarmed *state. If the sensor module has two channels for connecting two switches, two LEDs are available. Check which contact closure switch is in the "abnormal" status according to the channel number of the LED.*

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

Unmanaging Environmental Sensors

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the Branch Circuit Monitor device stops retrieving the sensor's reading and/or state.

To release a managed sensor:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 49).

   Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** *(on page 60).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to unmanage on the External Sensors page.
4. Click Release.

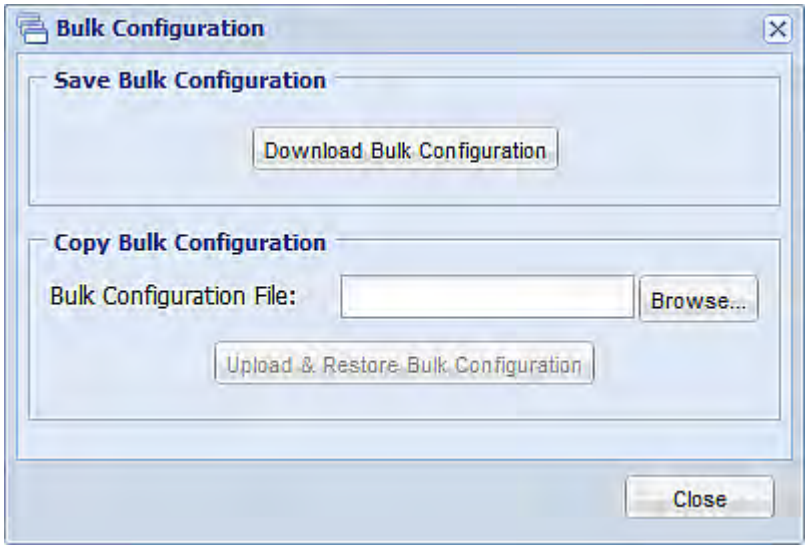
After a sensor is removed from management, the ID number assigned to that sensor is released and can be automatically assigned to any newly-detected sensor.

Copying Configurations with Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured Branch Circuit Monitor device to your PC. You can use this configuration file to:

- Copy that configuration to other Branch Circuit Monitor devices of the same model.
- Restore the settings of the same Branch Circuit Monitor device to previous configuration.

You must have the Administrator Privileges to save and copy the Branch Circuit Monitor configurations.



Saving a Branch Circuit Monitor Configuration

A source device is an already configured Branch Circuit Monitor device that is used to create a configuration file containing the settings that can be shared between Branch Circuit Monitor devices. These settings include user and role configurations, thresholds, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Mains channel name
- Branch circuit channel names
- Environmental sensor names
- Environmental sensor states and values
- SSL certificate

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the Branch Circuit Monitor devices in a different time zone than the source device.

To save a configuration file:

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Copying a Branch Circuit Monitor Configuration

A target device is a Branch Circuit Monitor device that loads another Branch Circuit Monitor device's configuration file.

Copying a Branch Circuit Monitor configuration to a target device adjusts that Branch Circuit Monitor device's settings to match those of the source Branch Circuit Monitor device. In order to successfully copy a Branch Circuit Monitor configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target Branch Circuit Monitor device must be of the same model type as the source Branch Circuit Monitor device.
- The target Branch Circuit Monitor device must be running the same firmware version as the source Branch Circuit Monitor device.

To copy a Branch Circuit Monitor Configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 150).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse and select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.
6. A message appears, prompting you to confirm the operation. Click Yes to confirm the operation.
7. Wait until the Branch Circuit Monitor device resets and the Login page re-appears, indicating that the configuration copy is complete.

Changing the Measurement Units

By default, the following measurement units are applied to all data shown in the Branch Circuit Monitor web interface:

- Temperature: degrees in Celsius (°C)
- Length or height: meters (m)
- Air pressure: pascal (pa)

The Branch Circuit Monitor web interface allows shows different measurement units based on the login name. That is, different users may see different measurement units displayed according to their preferences. The other alternatives for each measurement unit include:

- Temperature: degrees in Fahrenheit (°F)

- Length or height: feet (ft)
- Air pressure: psi

To change the measurement unit setting, you must have the administrator privileges.

To set the preferred measurement units:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Click the Preferences tab.
5. To change the temperature unit, select the desired option in the Temperature Unit field.
   - °C: This option displays the temperature in Celsius.
   - °F: This option displays the temperature in Fahrenheit.
6. To change the length or height unit, select the desired option in the Length Unit field.
   - Meter: This option displays the length or height in meters.
   - Feet: This option displays the length or height in feet.
7. To change the pressure unit, select the desired option in the Pressure Unit field.
   - Pascal: This option displays the pressure value in Pascals (Pa). A Pascal is equal to one newton per square meter.
   - psi: This option displays the pressure value in psi. Psi stands for pounds per square inch.
8. Click OK to save the changes.

Tip: You can determine the desired measurement unit when creating user profiles. See **Creating a User Profile** *(on page 88).*

Viewing the Webcam Images or Videos

If you connect a Logitech® QuickCam® Pro 9000 Webcam to the Branch Circuit Monitor device, you can visually monitor the environment close to the Branch Circuit Monitor. See ***Connecting a Logitech Webcam (Optional)*** (on page 32).

The Branch Circuit Monitor allows you to switch between static snapshots or animated videos captured by the webcam.

To view the images or videos:

1. Click the Webcam icon in the left pane.

   Note: A Webcam icon appears only when a Logitech® QuickCam® Pro 9000 Webcam is connected to the Branch Circuit Monitor. See **Connecting a Logitech Webcam (Optional)** *(on page 32).*

2. By default the Branch Circuit Monitor enters the snapshot mode. Wait around one minute for a snapshot to appear. In the snapshot mode, a snapshot mode icon appears on the top-left corner of the image.
   - To update the image with the latest snapshot, click the "Capture a snapshot" button.
   - To change the image resolution, select a different resolution from the drop-down list. The image is updated with the latest snapshot while the resolution changes.
3. To switch to the video mode, click the "Set video mode" button. The web interface shows the animated video captured by the webcam now. In the video mode, a video mode icon appears on the top-left corner of the image.
   - To change the video resolution, select a different resolution from the drop-down list.
4. To return to the snapshot mode, click the "Capture a snapshot" button.

Network Diagnostics

The Branch Circuit Monitor provides the following tools in the web interface for diagnosing potential networking issues.

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 292).*

Pinging a Host

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 10 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The Trace Route to Host dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. Click Run. A dialog appears, displaying the Trace Route results.
4. Click Close to quit the dialog.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP connections dialog appears.
2. Click Close to quit the dialog.

Viewing the Communication Log

The Branch Circuit Monitor allows you to inspect all communications occurred between the Branch Circuit Monitor device and its graphical user interface (GUI). The information is usually useful for a technical support engineer only and you may not need to view it.

This feature is accessible only by users with Administrative Privileges.

To view the communication log:

1. Choose Maintenance > View Communication Log. The Communication Log dialog appears.
2. The dialog shows the final page by default. You can:
   - Switch between different pages by doing one of the following:

     - Click ⏮ or ⏭ to go to the first or final page.

     - Click ◀ or ▶ to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.
   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » and select Show Details to view details.
3. To immediately update the communication log, click .
4. To save the communication log on your computer, click .
5. Enlarge the dialog if necessary. See ***Resizing a Dialog*** (on page 57).
6. You can re-sort the list or change the columns displayed. See ***Changing the View of a List*** (on page 55).
7. Click Close to quit the dialog.

Downloading Diagnostic Information

This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the Branch Circuit Monitor device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges.

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. The File Download dialog appears.

File Download
Do you want to open or save this file?
Name: diag-data.tgz
Type: WinRAR archive
From: 192.168.84.57
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

2. Click Save. The Save As dialog appears.
3. Navigate to the desired directory and click Save.
4. E-mail this file as instructed by Raritan Technical Support.

Firmware Upgrade

You may upgrade your Branch Circuit Monitor device to benefit from the latest enhancements, improvements and features.

The Branch Circuit Monitor firmware files are available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).

Updating the Branch Circuit Monitor Firmware

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the Branch Circuit Monitor device's firmware.

If applicable to your model, download the latest firmware file from the Raritan website, read the release notes, then start the upgrade. If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Warning: Do NOT perform the firmware upgrade over a wireless connection.

To update the firmware:

1. Choose Maintenance > Update Firmware. The Firmware Update dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

   Warning: Do NOT power off the Branch Circuit Monitor device during the update.

   During the firmware update:

   - A progress bar appears in the web interface, indicating the update status.
   - On the Branch Circuit Monitor device, the three-digit LED display shows “FUP.”
   - No users can successfully log in to the Branch Circuit Monitor.
   - In the web interface, all logged-in users see the Branch Circuit Monitor time out message, and the "disconnected" state is shown in the status bar.
   - The user management operation, if any, is forced to suspend.
7. When the update is complete, a message appears, indicating the update is successful.

8. The Branch Circuit Monitor device resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using the Branch Circuit Monitor with an SNMP manager, you should re-download the Branch Circuit Monitor MIB after the firmware update. This ensures your SNMP manager has the correct MIB for the latest release you are using. See *Using SNMP* (on page 155).

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the Branch Circuit Monitor device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

To view the firmware update history:

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.
   - Date and time of the firmware upgrade event
   - Previous firmware version
   - Update firmware version
   - Firmware upgrade result
2. You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 55).
3. To view the details of any firmware upgrade event, select it and click Details, or simply double-click the event. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the Branch Circuit Monitor device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate Branch Circuit Monitor firmware file is required in the recovery procedure.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the Branch Circuit Monitor User Guide (that is, the online help)

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the Branch Circuit Monitor device through the web interface.

To retrieve the embedded software packages information:

1. Choose Help > About Dominion PX. The About Dominion PX dialog appears, with a list of open source packages displayed.
2. You can click any link in the dialog to access related information or download any software package.

Browsing through the Online Help

The Branch Circuit Monitor User Guide is also provided in the form of online help, and accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

To use the Branch Circuit Monitor online help:

1. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:
   - To view the next topic, click the Next icon in the toolbar.
   - To view the previous topic, click the Previous icon.
   - To view the first topic, click the Home icon.
4. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow, and sub-topics appear below the topic.

- To collapse any expanded topic, click the black, gradient arrow ◢ prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow ▷, and all sub-topics below that topic disappear.

5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.
   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.
6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon in the toolbar.
9. To email your comments or suggestions regarding the user guide to Raritan, click the "Send feedback" icon.
10. To print the currently selected topic, click the "Print this page" icon.

Chapter 5 Using SNMP

This SNMP section helps you set up the Branch Circuit Monitor for use with an SNMP manager. The Branch Circuit Monitor can be configured to send traps to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

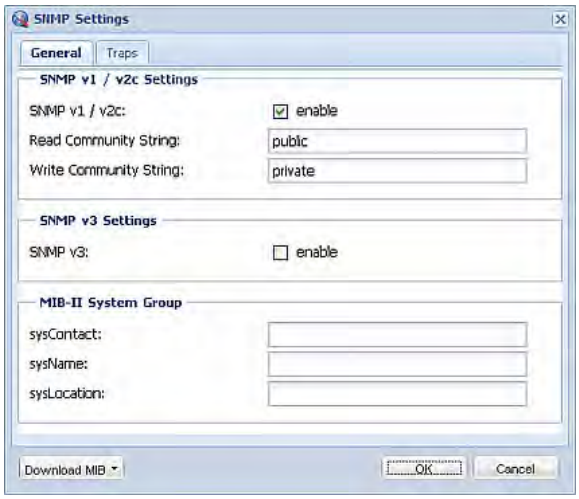
Enabling SNMP 155
Configuring Users for Encrypted SNMP v3 156
Configuring SNMP Traps.....157
SNMP Gets and Sets 158

Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on the Branch Circuit Monitor device.

To enable SNMP:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."

- Type the read/write community string in the Write Community String field. Usually the string is "private."

3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

Tip: You can permit or disallow a user to access the Branch Circuit Monitor via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 156).*

4. Type the SNMP MIB-II sysContact value in the sysContact field.
5. Type the SNMP MIB-II sysName value in the sysName field.
6. Type the SNMP MIB-II sysLocation value in the sysLocation field.
7. Click OK to save the changes.

Important: You must download the SNMP MIB for your Branch Circuit Monitor to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see *Downloading SNMP MIB* **(on page 158).**

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the Branch Circuit Monitor.

To configure users for SNMP v3 encrypted communication:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 88).
5. Click OK to save the changes. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Traps

The Branch Circuit Monitor automatically keeps an internal log of events that occur. See ***Configuring Event Rules*** (on page 118). These events can also be used to send SNMP traps to a third party manager.

To configure the Branch Circuit Monitor to send SNMP traps:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the System SNMP Trap Rule.
3. Select the Enabled checkbox to enable this event rule.
4. Click Save to save the changes.
5. Click the Actions tab if you have not configured the SNMP trap actions.
6. Select System SNMP Trap Action to set up the trap destinations.
7. Type an IP address in the Host 1 field. This is the address to which traps are sent by the SNMP system agent.
8. Type the communication port number in the Port 1 field.
9. Type the name of the SNMP community in the Community field. The community is the group representing the Branch Circuit Monitor and all SNMP management stations.
10. To specify more than one SNMP trap destination, repeat Steps 8 to 10 for additional destinations. A maximum of 3 destinations can be specified.
11. Click Save to save the changes.
12. Click Close to quit the dialog.

Note: You should update the MIB used by your SNMP manager when updating to a new Branch Circuit Monitor release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 158).*

SNMP Gets and Sets

In addition to sending traps, the Branch Circuit Monitor is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the Branch Circuit Monitor, such as the system location, and the current on a specific branch circuit.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the Branch Circuit Monitor device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The Branch Circuit Monitor does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom Branch Circuit Monitor MIB.

The Branch Circuit Monitor MIB

The SNMP MIB file is required for using your Branch Circuit Monitor device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the Branch Circuit Monitor can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

To download the file from the SNMP Settings dialog:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appear.
3. Select the desired MIB file to download.
   - PDU-MIB: The SNMP MIB file for Branch Circuit Monitor's power management.
4. Click Save to save the file onto your computer.

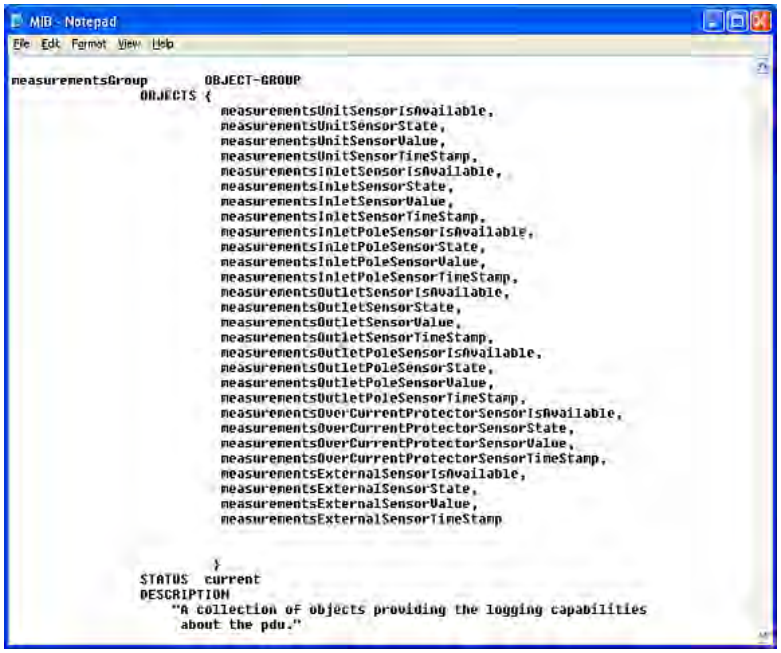
To download the file from the Device Information dialog:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the "download" link in the PDU-MIB field to download the desired SNMP MIB file.
   - PDU-MIB: The SNMP MIB file for Branch Circuit Monitor's power management.
3. Click Save to save the file onto your computer.

Layout

Opening the MIB reveals the custom objects that describe the Branch Circuit Monitor system at the unit level as well as at the individual branch circuit level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for sensor readings of Branch Circuit Monitor as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the device's current rating.

Note that the MIB file uses the following terms to refer to the device or its components:

- pdu, px or unit: The Branch Circuit Monitor device
- inlet: Mains channels
- outlet: Branch circuit channels

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the Branch Circuit Monitor to generate a warning and send an SNMP trap when certain parameters are exceeded. See ***Setting Power Thresholds*** (on page 83) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 6 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a Branch Circuit Monitor device.

In This Chapter

About the Interface 161
Logging in to CLI 161
Help Command 164
Showing Information 165
Configuring the Branch Circuit Monitor Device and Network 180
Unblocking a User 291
Resetting the Branch Circuit Monitor 291
Network Troubleshooting 292
Querying Available Parameters for a Command 296
Retrieving Previous Commands 296
Automatically Completing a Command 296
Logging out of CLI 297

About the Interface

The Branch Circuit Monitor provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the Branch Circuit Monitor device
- Display the Branch Circuit Monitor and network information, such as the device name, firmware version, IP address, and so on
- Configure the Branch Circuit Monitor and network settings
- Troubleshoot network problems

You can access the interface over a serial connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying the Network Service Settings** *(on page 66).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

To log in using HyperTerminal:

1. Connect your computer to the Branch Circuit Monitor device via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

   Make sure the COM port settings use this configuration:

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the Branch Circuit Monitor by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion Serial Console" under the Ports group.

3. Press Enter. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters. Then you are prompted to enter a password.

   ```
   Username: admin
   Password: _
   ```

5. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 164) for details.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the Branch Circuit Monitor web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the Branch Circuit Monitor device.

With SSH or Telnet

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See ***Modifying the Network Service Settings*** (on page 66).
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as:
```

3. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters.

Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password:
```

4. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.
5. After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 164) for details.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the Branch Circuit Monitor web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the Branch Circuit Monitor device.

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who does not have full permissions to configure the Branch Circuit Monitor device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the Branch Circuit Monitor device, the # prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator mode. In this mode, the prompt changes to **config:#** and you can change Branch Circuit Monitor device and network configurations. See ***Entering the Configuration Mode*** (on page 181).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator mode. In this mode, the prompt changes to **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See ***Entering the Diagnostic Mode*** (on page 292).

Closing a Serial Connection

Close the window or terminal emulation program when you finish accessing a Branch Circuit Monitor device over the serial connection.

When accessing or upgrading multiple Branch Circuit Monitor devices, do not transfer the serial cable from one device to another without closing the serial connection window first.

Help Command

The help command shows a list of main CLI commands. This is helpful when you are not familiar with the commands.

▶ **The help command syntax is:**

```
#      help
```

Press Enter after typing the command, and a list of main commands is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding a question mark to the end of the command. See **Querying Available Parameters for a Command** *(on page 296).*

Showing Information

You can use the show commands to view current settings or status of the Branch Circuit Monitor device or part of it, such as the IP address, networking mode, firmware version, circuit breaker state, inlet ratings, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
#       show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
#       show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both of IPv4 and IPv6 settings. *Tip: You can also type the command without adding this option "all" to get the same data.*
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, such as LAN interface speed, duplex mode, and current LAN interface status.

```
#       show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
#       show network mode
```

Wireless Configuration

This command only shows the wireless configuration of the Branch Circuit Monitor device, such as the SSID parameter.

```
#       show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS and SSH services, and SNMP settings.

```
#       show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh* and *snmp*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.

Device Configuration

This command shows the Branch Circuit Monitor's configuration, such as the device name, firmware version and model type.

```
#       show bcm
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show bcm details
```

Branch Circuit Information

This command syntax shows the branch circuit information.

```
#        show branches <n>
```

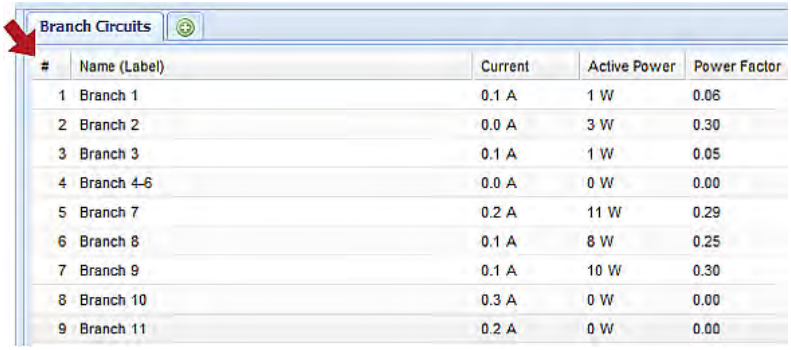
To show detailed information, add the parameter "details" to the end of the command.

```
#        show branches <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all branch circuits. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific branch circuit number	Displays the information for the specified branch circuit only. • <n> is the index number of the desired branch circuit channel. This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor. See the figure below.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

Displayed information:

- Without the parameter "details," only the branch circuit name is displayed.
- With the parameter "details," more branch circuit information is displayed in addition to the name, such as the RMS current, voltage and active energy.

Mains Information

This command syntax shows the mains information.

```
#        show mains
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show mains details
```

Displayed information:

- Without the parameter "details," only the mains' name and current values are displayed.
- With the parameter "details," more mains information is displayed in addition to the current values, such as the voltage, active power and active energy.

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show externalsensors <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the Branch Circuit Monitor web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A discrete (on/off) sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number and X, Y, and Z coordinates.

Branch Circuit Threshold Information

This command syntax shows the specified branch circuit sensor's threshold-related information.

```
#       show sensor branch <n> <sensor type>
```

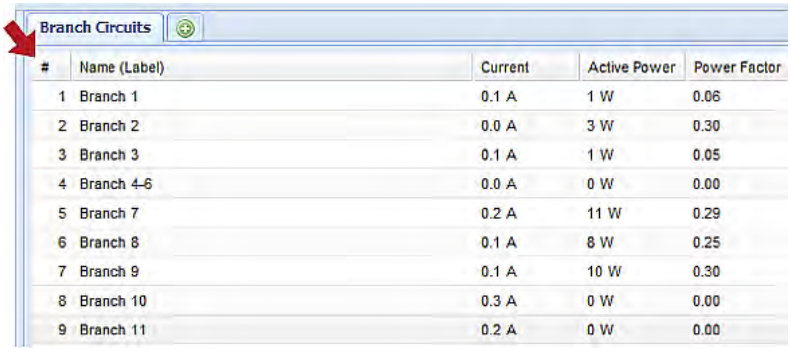
To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor branch <n> <sensor type> details
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified branch circuit sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Not available" is displayed.

Branch Circuit Pole Threshold Information

This command is applicable to a three-phase branch circuit only. See ***Configuring the Branch Circuit Channels*** (on page 77) for how to configure a 3-phase branch circuit.

This command syntax shows the specified branch circuit pole sensor's threshold-related information.

```
#       show sensor branchpole <n> <p> <sensor type>
```

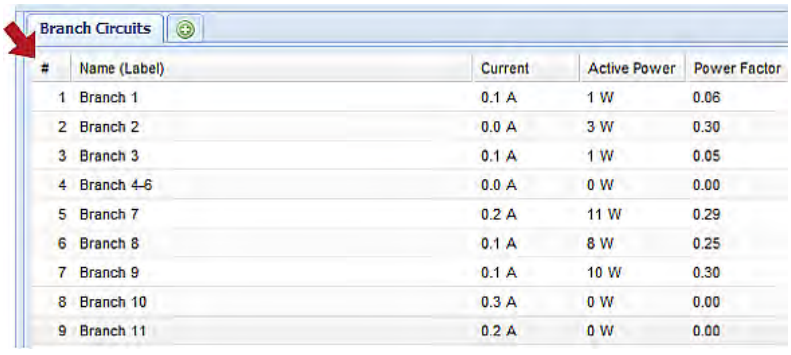
To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor branchpole <n> <p> <sensor type> details
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <p> is the label of the branch circuit pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified branch circuit pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Not available" is displayed.

Mains Threshold Information

This command syntax shows the specified mains sensor's threshold-related information.

```
#       show sensor mains <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor mains <sensor type> details
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified mains sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Not available" is displayed.

Mains Pole Threshold Information

This command is applicable to a three-phase power system only.

This command syntax shows the specified mains pole sensor's threshold-related information.

```
#       show sensor mainspole <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor mainspole <p> <sensor type> details
```

Variables:

- <p> is the label of the mains pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified mains pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Not available" is displayed.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#       show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor externalsensor <n> details
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the Branch Circuit Monitor web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Security Settings

This command shows the security settings of the Branch Circuit Monitor.

```
#       show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time and user idle timeout.

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#       show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, "enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred temperature unit and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#       show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

EnergyWise Settings

This command shows the Branch Circuit Monitor's current configuration for Cisco® EnergyWise.

```
#       show energywise
```

Reliability Data

This command shows the reliability data.

```
#       show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#       show reliability errorlog <n>
```

Variables:

- <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Command History

This command syntax shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing the history commands.

```
#       show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Configuring the Branch Circuit Monitor Device and Network

To configure the Branch Circuit Monitor device or network settings through the CLI, you must log in as the administrator.

Entering the Configuration Mode

You must enter the configuration mode since configuration commands function in the configuration mode only.

To enter the configuration mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.

   Note: If you enter the configuration mode from the user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** *(on page 164).*

2. Type `config` and press Enter. The config:# prompt appears, indicating that you have entered the configuration mode.

   ```
   config:# _
   ```

3. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes. See *Quitting the Configuration Mode* **(on page 290).**

Device Configuration Commands

A device configuration command begins with *bcm*. You can use the device configuration commands to change the settings that apply to the whole Branch Circuit Monitor.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the Device Name

This command syntax changes the Branch Circuit Monitor device's name.

```
config:#   bcm name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "my bcm2400" to the Branch Circuit Monitor.

```
config:#   bcm name "my bcm2400"
```

Enabling or Disabling Data Logging

This command syntax enables or disables the data logging feature.

```
config:#   bcm dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see ***Setting Data Logging*** (on page 73).

Example

The following command enables the data logging feature.

```
config:#   bcm dataRetrieval enable
```

Setting the Data Logging Measurements Per Entry

This command syntax defines the number of measurements accumulated per log entry.

```
config:#   bcm measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see ***Setting Data Logging*** (on page 73).

Example

The following command determines that 66 measurements are accumulated per log entry for sensors, that is, 66 seconds.

```
config:#   bcm measurementsPerLogEntry 66
```

Specifying the Device Altitude

This command syntax specifies your Branch Circuit Monitor device's altitude above sea level (in meters). You must specify the Branch Circuit Monitor device's altitude above sea level if a Raritan differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 315).

```
config:#   bcm deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Example

The following command determines that the Branch Circuit Monitor device is located at 1500 meters above sea level.

```
config:#   bcm deviceAltitude 1500
```

Setting the Z Coordinate Format for Environmental Sensors

This command syntax enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   bcm externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.

Option	Description
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** *(on page 231).*

Example

The following command determines that the unit of rack is used for specifying the Z coordinate of environmental sensors.

```
config:#   bcm externalSensorsZCoordinateFormat rackUnits
```

Networking Configuration Commands

A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Setting the Networking Mode

If your Branch Circuit Monitor device is implemented with both of the wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command syntax enables the wired or wireless networking mode.

```
config:#   network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the Branch Circuit Monitor does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Example

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your Branch Circuit Monitor device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command syntax determines which IP protocol is enabled on the Branch Circuit Monitor.

```
config:#   network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Example

The following command determines that both of IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Selecting IPv4 or IPv6 Addresses

This command syntax determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both of IPv4 and IPv6 protocols are enabled on the Branch Circuit Monitor.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Example

The following command determines that only IPv4 addresses returned by the DNS server are used.

```
config:#   network ip dnsResolverPreference preferV4
```

Setting the Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the SSID

This command syntax specifies the SSID string.

```
config:#   network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

The following command assigns "myssid" as the SSID.

```
config:#   network wireless SSID myssid
```

Setting the Authentication Method

This command syntax sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Example

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command syntax.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

This command assigns "encryp-key" as the PSK.

```
config:#   network wireless PSK encryp-key
```

Setting the EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

Setting the Outer Authentication

This command syntax determines the outer authentication protocol for the EAP.

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

Variables:

- The value of <outer_auth> is *PEAP* because Branch Circuit Monitor only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.

Example

The following command determines the outer authentication protocol for the EAP authentication is Protected Extensible Authentication Protocol (PEAP).

```
config:#   network wireless eapOuterAuthentication PEAP
```

Setting the Inner Authentication

This command syntax determines the inner authentication protocol for the EAP.

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

Variables:

- The value of <inner_auth> is *MSCHAPv2* because Branch Circuit Monitor only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.

Example

The following command determines the inner authentication protocol for the EAP authentication is MSCHAPv2.

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

Setting the EAP Identity

This command syntax determines the EAP identity.

```
config:#   network wireless eapIdentity <identity>
```

Variables:

- <identity> is your user name for the EAP authentication.

Example

The following command sets the EAP identity to "eap_user01."

```
config:#   network wireless eapIdentity eap_user01
```

Setting the EAP Password

This command syntax determines the EAP password.

```
config:#   network wireless eapPassword
```

Variables:

- <password> is your password for EAP authentication.

Example

The following command sets the EAP password to "user01_password."

```
config:#   network wireless eapPassword user01_password
```

Providing the EAP CA Certificate

You may need to provide a third-party CA certificate for the EAP authentication.

To provide a CA certificate:

1. Type the CA certificate command as shown below and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

2. The system prompts you to enter the contents of the CA certificate. Do the following to input the contents:
   a. Open your CA certificate with a text editor.
   b. Copy the contents between the "--- BEGIN CERTIFICATE ---" and "--- END CERTIFICATE ---" lines in a certificate.
   c. Paste the certificate contents into the terminal.
   d. Press Enter.

   Tip: To remove an existing CA certificate, simply press Enter without typing or pasting anything when the system prompts you to input the certificate contents.

3. If the certificate is valid, the system shows the command prompt "`config:#`" again. If not, it shows a message indicating that the certificate is not valid.

Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 181).
2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE" as illustrated below.

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

   ```
   config:#
   ```

Setting the BSSID

This command syntax specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is the MAC address of the wireless access point.

Example

The following command specifies that the BSSID is 00:14:6C:7E:43:81.

```
config:#   network wireless BSSID 00:14:6C:7E:43:81
```

Configuring the IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Example

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Setting the Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command syntax:

```
config:#   network ipv4 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Example

The following command sets the preferred host name to "my-host."

```
config:#   network ipv4 preferredHostName my-host
```

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the Branch Circuit Monitor device.

```
config:#   network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your Branch Circuit Monitor device. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command assigns the static IPv4 address "192.168.84.222" to the Branch Circuit Monitor device.

```
config:#   network ipv4 ipAddress 192.168.84.222
```

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command syntax to define the subnet mask.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the subnet mask to 192.168.84.0.

```
config:#   network ipv4 subnetMask 192.168.84.0
```

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the IPv4 gateway to 255.255.255.0.

```
config:#   network ipv4 gateway 255.255.255.0
```

Setting the IPv4 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server.

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command determines that the primary DNS server is 192.168.84.30.

```
config:#   network ipv4 primaryDNSServer 192.168.84.30
```

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server.

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Note: The Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 192.168.84.33.

```
config:#   network ipv4 secondaryDNSServer 192.168.84.33
```

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS enable
```

Configuring the IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Example

The following command sets the IP configuration mode to the static IP address mode.

```
config:#   network ipv6 ipConfigurationMode static
```

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the Branch Circuit Monitor device.

```
config:#   network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your Branch Circuit Monitor device. This value uses the IPv6 address format.

Example

The following command assigns the static IPv6 address "3210:4179:0:8:0:800:200C:417A" to the Branch Circuit Monitor device.

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Example

The following command sets the gateway to 500:0:330:0:4:9:3:2.

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

Setting the IPv6 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 200).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Example

The following command determines that the primary DNS server is 2103:288:8201:1::14.

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 200).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

Note: The Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 2103:288:8201:1::700.

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS enable
```

Setting the LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the LAN Interface Speed

This command syntax determines the LAN interface speed.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.

Option	Description
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Example

The following command lets the Branch Circuit Monitor determine the optimal LAN interface speed through auto-negotiation.

```
config:#   network interface LANInterfaceSpeed auto
```

Changing the LAN Duplex Mode

This command syntax determines the LAN interface duplex mode.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The Branch Circuit Monitor selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the Branch Circuit Monitor device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Example

The following command lets the Branch Circuit Monitor determine the optimal transmission mode through auto-negotiation.

```
config:#   network interface LANInterfaceDuplexMode auto
```

Setting the Network Service Parameters

A network service command begins with *network services*.

Changing the HTTP Port

This command syntax changes the HTTP port.

```
config:#   network services http <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

Example

The following command sets the HTTP port to 81.

```
config:#   network services http 81
```

Changing the HTTPS Port

This command syntax changes the HTTPS port.

```
config:#   network services https <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.

Example

The following command sets the HTTPS port to 333.

```
config:#   network services https 333
```

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command syntax enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Example

The following command enables the Telnet service.

```
config:#   network services telnet enabled true
```

Changing the Telnet Port

This command syntax changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Example

The following command syntax sets the TCP port for Telnet to 44.

```
config:#   network services telnet port 44
```

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command syntax enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Example

The following command enables the SSH service.

```
config:#   network services ssh enabled true
```

Changing the SSH Port

This command syntax changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Example

The following command syntax sets the TCP port for SSH to 555.

```
config:#   network services ssh port 555
```

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command syntax enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Example

The following command enables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c enable
```

Enabling or Disabling SNMP v3

This command syntax enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Example

The following command enables the SNMP v3 protocol.

```
config:#   network services snmp v3 enable
```

Setting the SNMP Read Community

This command syntax sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

This command syntax sets the SNMP read-only community string to "public."

```
config:#   network services snmp readCommunity public
```

Setting the SNMP Write Community

This command syntax sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

The following command sets the SNMP read/write community string to "private."

```
config:#   network services snmp writeCommunity private
```

Setting the sysContact Value

This command syntax sets the SNMP sysContact MIB-II value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysContact to "John_Krause."

```
config:#   network services snmp sysContact John_Krause
```

Setting the sysName Value

This command syntax sets the SNMP sysName MIB-II value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysName to "Win7_system"

```
config:#   network services snmp sysName Win7_system
```

Setting the sysLocation Value

This command syntax sets the SNMP sysLocation MIB-II value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysLocation to "New_TAIPEI"

```
config:#   network services snmp sysLocation New_TAIPEI
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the Branch Circuit Monitor device from specific or a range of IP addresses.

A firewall configuration command begins with *security ipAccessControl*.

Modifying the Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- **To enable or disable the firewall control feature, use this command syntax:**

```
config:#   security ipAccessControl enabled <option>
```

- **To determine the default firewall control policy, use this command syntax:**

```
config:#   security ipAccessControl defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets up two parameters of the IP access control feature.

```
config:#   security ipAccessControl enabled true defaultPolicy accept
```

Results:

- The IP access control feature is enabled.
- The default policy is set to "accept."

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command syntax for adding a rule varies.

▶ **To add a new rule to the bottom of the rules list, use this command syntax:**

```
config:#   security ipAccessControl rule add <ip_mask> <policy>
```

▶ **To add a new rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#   security ipAccessControl rule add <ip_mask> <policy> <insert> <rule_number>
```

-- OR --

```
config:#   security ipAccessControl rule add <insert> <rule_number> <ip_mask> <policy>
```

Variables:

- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.

Policy	Description
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command adds a new IP access control rule and specifies its location in the list.

```
config:#   security ipAccessControl rule add 192.168.84.123/24 accept insertAbove 5
```

Results:

- A new firewall control rule is added, allowing all packets from the IP address 192.168.84.123 to be accepted.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands. A firewall control rule command begins with *security ipAccessControl rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command syntax for adding a rule varies.

- **To add a new rule to the bottom of the rules list, use this command syntax:**

```
config:#    security ipAccessControl rule add <ip_mask> <policy>
```

- **To add a new rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#    security ipAccessControl rule add <ip_mask> <policy> <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl rule add <insert> <rule_number> <ip_mask> <policy>
```

Variables:

- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command adds a new IP access control rule and specifies its location in the list.

```
config:#   security ipAccessControl rule add 192.168.84.123/24 accept insertAbove 5
```

Results:

- A new firewall control rule is added, allowing all packets from the IP address 192.168.84.123 to be accepted.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command syntax varies.

- **The command syntax to modify a rule's IP address and/or subnet mask:**

```
config:#   security ipAccessControl rule modify <rule_number> ipMask <ip_mask>
```

- **The command syntax to modify a rule's policy:**

```
config:#   security ipAccessControl rule modify <rule_number> policy <policy>
```

- **The command syntax to modify all contents of an existing rule:**

```
config:#    security ipAccessControl rule modify <rule_number> ipMask <ip_mask> policy
            <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

Example

The following command modifies all contents of the 5th rule.

```
config:#    security ipAccessControl rule modify 5 ipMask 192.168.84.123/24 policy
            accept
```

Results:

- The IP address is changed to 192.168.84.123, and the subnet mask to 255.255.255.0.
- The policy now becomes "accept."

Deleting a Firewall Rule

This command removes a specific rule from the list.

```
config:#   security ipAccessControl rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 5th rule from the IP access control list.

```
config:#   security ipAccessControl rule delete 5
```

HTTPS Access

This command determines whether the HTTPS access to the Branch Circuit Monitor web interface is forced. If yes, all HTTP access attempts are automatically directed to HTTPS.

```
config:#   security enforceHttpsForWebAccess <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the HTTPS access to the web interface.
disable	Disables the HTTPS access to the web interface.

Example

The following command disables the HTTPS access feature.

```
config:#   security enforceHttpsForWebAccess disable
```

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before being forced to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify the login limitation parameters at a time. See ***Multi-Command Syntax*** (on page 289).

Single Login Limitation

This command syntax enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Example

The following command disables the single login feature so that more than one user can log in using the same user name at the same time.

```
config:#   security loginLimits singleLogin disable
```

Password Aging

This command syntax enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:#   security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Example

The following command enables the password aging feature.

```
config:#   security loginLimits passwordAging enable
```

Password Aging Interval

This command syntax determines how often the password should be changed.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Example

The following command sets the password again interval to 90 days.

```
config:#   security loginLimits passwordAgingInterval 90
```

Idle Timeout

This command syntax determines how long a user can remain idle before that user is forced to log out of the Branch Circuit Monitor web interface.

```
config:#   security loginLimits idleTimeout <value>
```

Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

Example

The following command sets the idle timeout to 10 munites.

```
config:#   security loginLimits idleTimeout 10
```

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

- **To determine the maximum number of failed logins before blocking a user, use this command syntax:**

```
config:#   security userBlocking maximumNumberOfFailedLogins <value1>
```

- **To determine how long a user's login is blocked, use this command syntax:**

```
config:#   security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value in minutes.

Tip: You can combine multiple commands to modify the user blocking parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets up two user blocking parameters.

```
config:#   security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See ***Multi-Command Syntax*** (on page 289).

Enabling or Disabling Strong Passwords

This command syntax enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Example

This command syntax enables the strong password feature.

```
config:#   security strongPasswords enabled true
```

Minimum Password Length

This command syntax determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Example

This command syntax determines a password must comprise at least 8 characters.

```
config:#   security strongPasswords minimumLength 8
```

Maximum Password Length

This command syntax determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Example

This command syntax determines that a password must NOT comprise more thant 20 characters.

```
config:#   security strongPasswords maximumLength 20
```

Lowercase Character Requirement

This command syntax determines whether a strong password includes at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Example

This command syntax determines that a password must include at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

Uppercase Character Requirement

This command syntax determines whether a strong password includes at least a uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Example

This command determines a password must comprise at least one uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

Numeric Character Requirement

This command syntax determines whether a strong password includes at least a numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Example

The following command determines that a password must comprise at least one numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

Special Character Requirement

This command syntax determines whether a strong password includes at least a special character.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Example

The following command determines that a password must comprise at least one special character.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

Maximum Password History

This command syntax determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Example

The following command determines that the previous 7 passwords CANNOT be re-used when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth 7
```

Role-Bassed Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

A role-based access control command begins with *security roleBasedAccessControl*.

Modifying the Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- **To enable or disable the role-based access control feature, use this command syntax:**

```
config:#   security roleBasedAccessControl enabled <option>
```

- **To determine the role-based access control policy, use this command syntax:**

```
config:#   security roleBasedAccessControl defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets two parameters of the role-based IP access control feature.

```
config:#   security roleBasedAccessControl enabled true defaultPolicy allow
```

Results:

- The role-based IP access control feature is enabled.
- The default policy is set to "allow."

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

A role-based access control command for managing rules begins with *security roleBasedAccessControl rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

▶ **To add a new rule to the bottom of the rules list, use this command syntax:**

```
config:#   security roleBasedAccessControl rule add <start_ip> <end_ip> <role> <policy>
```

▶ **To add a new rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#   security roleBasedAccessControl rule add <start_ip> <end_ip> <role> <policy>
           <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command creates a new role-based access control rule and specifies its location in the list.

```
config:#    security roleBasedAccessControl rule add 192.168.78.50 192.168.90.100 admin
            deny insertAbove 3
```

Results:

- A new role-based access control rule is added, dropping all packets from any IP address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

To modify a rule's IP address range, use this command syntax:

```
config:#    security roleBasedAccessControl rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

To modify a rule's role, use this command syntax:

```
config:#    security roleBasedAccessControl rule modify <rule_number> role <role>
```

To modify a rule's policy, use this command syntax:

```
config:#    security roleBasedAccessControl rule modify <rule_number> policy <policy>
```

To modify all contents of an existing rule, use this command syntax:

```
config:#    security roleBasedAccessControl rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Example

The following command modifies all contents of the 8th rule.

```
config:#    security roleBasedAccessControl rule modify 8
            startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
            policy allow
```

Results:

- The starting IP address is changed to 192.168.8.8, and the ending IP address to 192.168.90.90.
- The role is changed to "operator."
- The policy now becomes "allow."

Deleting a Role-Based Access Control Rule

This command removes a specific rule from the list.

```
config:#   security roleBasedAccessControl rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 7th rule.

```
config:#   security roleBasedAccessControl rule delete 7
```

Branch Circuit Channel Configuration Commands

A branch circuit channel configuration command begins with *branch*. Such a command allows you to configure an individual branch circuit channel.

Changing the Branch Circuit Channel Name

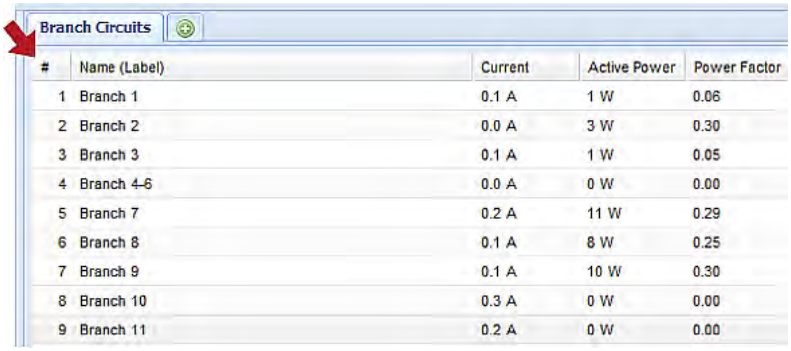
This command syntax names a branch circuit channel.

```
config:#   branch <n> name "<name>"
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Air conditioner" to the branch circuit channel #8.

```
config:#   branch 8 name "Air conditioner"
```

Mains Channel Configuration Commands

A mains configuration command begins with *mains*. You can configure the mains channels by using the mains configuration command.

Changing the Inlet Name

This command syntax names the mains channel(s).

```
config:#   mains name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Server room" to the mains channel(s).

```
config:#   mains name "Server room"
```

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Changing the Sensor Name

This command syntax names an environmental sensor.

```
config:#   externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Specifying the Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party detectors/switches, and you must specify the type of connected detector/switch for proper operation. Use this command syntax when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.

Type	Description
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Example

The following indicates that a smoke detector is being connected to Raritan's contact closure sensor (DPX-CC2-TR) whose ID number shown in the Branch Circuit Monitor web interface is 2.

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

Setting the X Coordinate

This command syntax specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 2nd cabinet" to the X coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Setting the Y Coordinate

This command syntax specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 4th row" to the Y coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Setting the Z Coordinate

This command syntax specifies the Z coordinate of an environmental sensor.

config:# externalsensor <n> zlabel "<coordinate>"

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units. See **Setting the Z Coordinate Format for Environmental Sensors** *(on page 183).*

Example

The following command sets the value "The 5th rack" to the Z coordinate of the environmental sensor with the ID number 4 after the Z coordinate's format is set to *freeForm*.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Changing the Sensor Description

This command syntax provides a description for a specific environmental sensor.

```
config:#   externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command gives the description "humidity detection" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 description "humidity detection"
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Mains channels
- Mains poles (for three-phase monitors)
- Branch circuit channels
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold is being enabled.

Commands for Branch Circuit Sensors

A sensor configuration command for branch circuit channels begins with *sensor branch*.

Setting the Branch Circuit Channel's Upper Critical Threshold

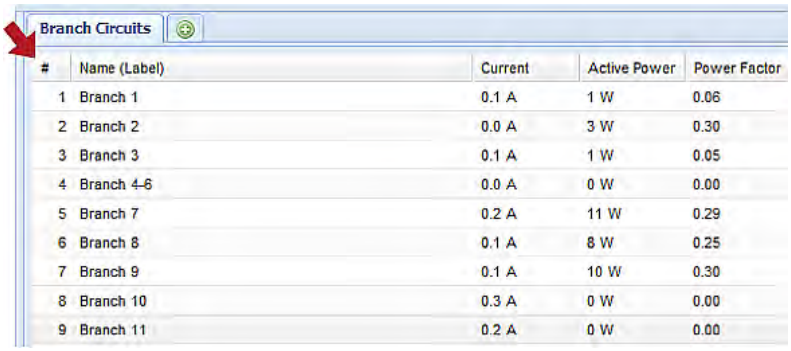
This command syntax configures the Upper Critical threshold of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Sensor type	Description
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified branch circuit channel.
disable	Disables the upper critical threshold for the specified branch circuit channel.
A numeric value	Sets a value for the upper critical threshold of the specified branch circuit channel and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold of the branch circuit #5's RMS current to 20A. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor branch 5 current upperCritical 20
```

Setting the Branch Circuit Channel's Upper Warning Threshold

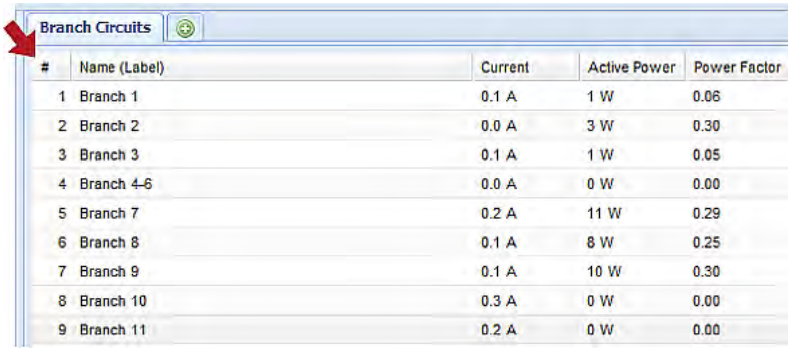
This command syntax configures the Upper Warning threshold of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified branch circuit channel.

Option	Description
disable	Disables the upper warning threshold for the specified branch circuit channel.
A numeric value	Sets a value for the upper warning threshold of the specified branch circuit channel and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold of the branch circuit #5's RMS current.

```
config:#   sensor branch 5 current upperWarning enable
```

Setting the Branch Circuit Channel's Lower Critical Threshold

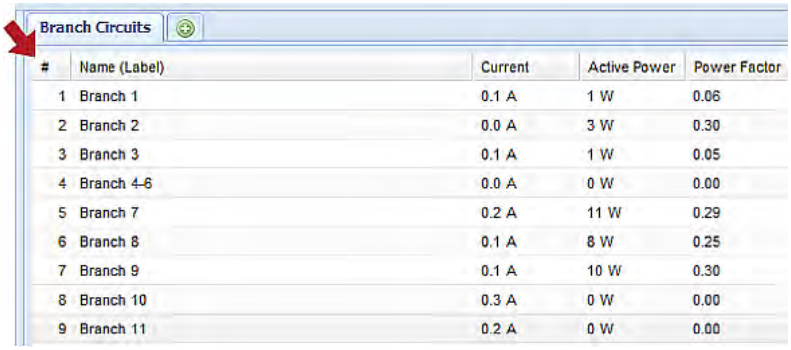
This command syntax configures the Lower Critical threshold of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.


Branch Circuits
Name (Label) Current Active Power Power Factor
1 Branch 1 0.1 A 1 W 0.06
2 Branch 2 0.0 A 3 W 0.30
3 Branch 3 0.1 A 1 W 0.05
4 Branch 4-6 0.0 A 0 W 0.00
5 Branch 7 0.2 A 11 W 0.29
6 Branch 8 0.1 A 8 W 0.25
7 Branch 9 0.1 A 10 W 0.30
8 Branch 10 0.3 A 0 W 0.00
9 Branch 11 0.2 A 0 W 0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified branch circuit channel.
disable	Disables the lower critical threshold for the specified branch circuit channel.
A numeric value	Sets a value for the lower critical threshold of the specified branch circuit channel and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold for the branch circuit #5's RMS current to 10A. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor branch 5 current lowerCritical 10
```

Setting the Branch Circuit Channel's Lower Warning Threshold

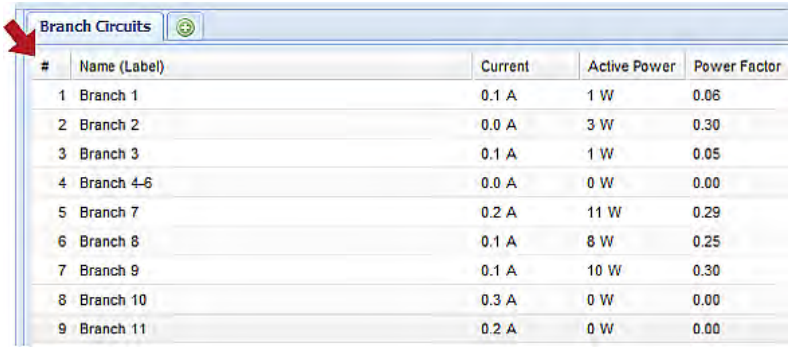
This command syntax configures the Lower Warning threshold of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified branch circuit channel.

Option	Description
disable	Disables the lower warning threshold for the specified branch circuit channel.
A numeric value	Sets a value for the lower warning threshold of the specified branch circuit channel and enables this threshold at the same time.

Example

The following command disables the Lower Warning threshold for the branch circuit #5's RMS current.

```
config:#   sensor branch 5 current lowerWarning disable
```

Setting the Branch Circuit Channel's Deassertion Hysteresis

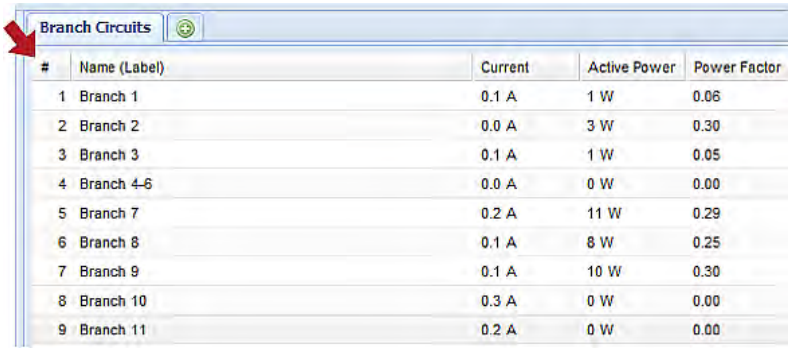
This command syntax configures the deassertion hysteresis value of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified branch circuit channel. See ***What is Deassertion Hysteresis?*** (on page 86) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the branch circuit #5's RMS current to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor branch 5 current hysteresis 0.2
```

Setting the Branch Circuit Channel's Assertion Timeout

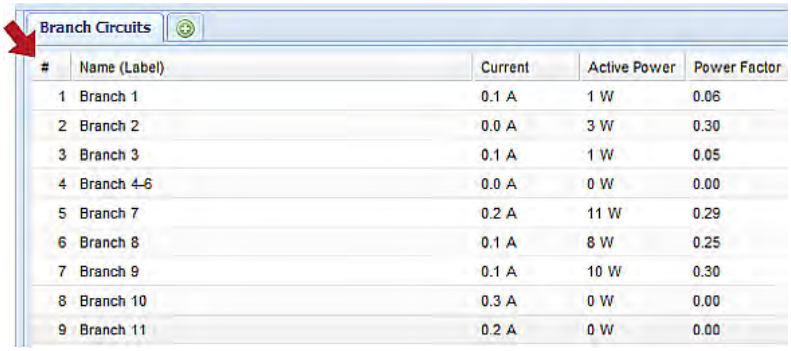
This command syntax configures the assertion timeout value of a branch circuit channel.

```
config:#   sensor branch <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified branch circuit channel. See ***What is Assertion Timeout?*** (on page 88).

Example

The following command sets the assertion timeout value of the branch circuit #5's RMS current to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor branch 5 current assertionTimeout 4
```

Commands for Branch Circuit Pole Sensors

A sensor configuration command for branch circuit poles begins with *sensor branchpole*. This type of command is available on a 3-phase branch circuit only. See ***Configuring the Branch Circuit Channels*** (on page 77) for how to configure a 3-phase branch circuit.

Setting the Upper Critical Threshold for a Branch Circuit Pole

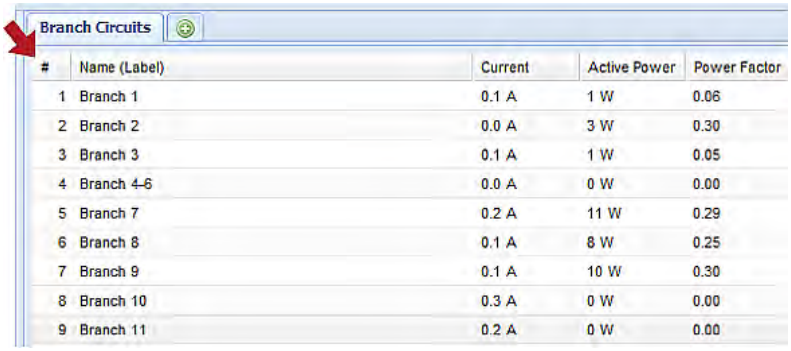
This command syntax configures the Upper Critical threshold of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> upperCritical <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.


Branch Circuits
Name (Label) Current Active Power Power Factor
1 Branch 1 0.1 A 1 W 0.06
2 Branch 2 0.0 A 3 W 0.30
3 Branch 3 0.1 A 1 W 0.05
4 Branch 4-6 0.0 A 0 W 0.00
5 Branch 7 0.2 A 11 W 0.29
6 Branch 8 0.1 A 8 W 0.25
7 Branch 9 0.1 A 10 W 0.30
8 Branch 10 0.3 A 0 W 0.00
9 Branch 11 0.2 A 0 W 0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3

Pole	Label <p>	Current sensor	Voltage sensor
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified branch circuit pole.
disable	Disables the upper critical threshold for the specified branch circuit pole.
A numeric value	Sets a value for the upper critical threshold of the specified branch circuit pole and enables this threshold at the same time.

Example

The following command disables the Upper Critical threshold for the pole 3 (L3-L1) voltage of the branch circuit #4.

```
config:#   sensor branchpole 4 L3 voltage upperCritical disable
```

Setting the Upper Warning Threshold for a Branch Circuit Pole

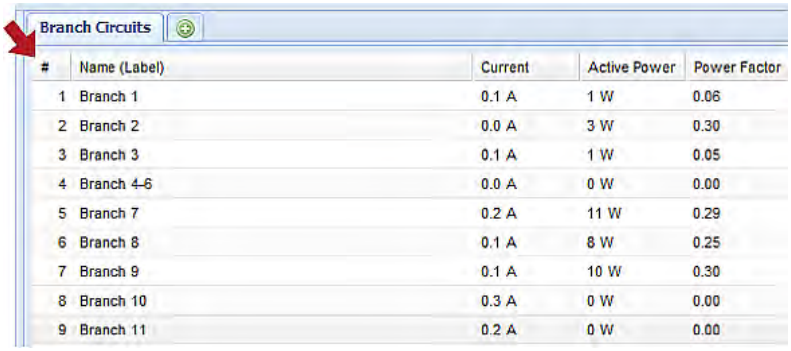
This command syntax configures the Upper Warning threshold of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> upperWarning <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.


Branch Circuits
Name (Label) Current Active Power Power Factor
1 Branch 1 0.1 A 1 W 0.06
2 Branch 2 0.0 A 3 W 0.30
3 Branch 3 0.1 A 1 W 0.05
4 Branch 4-6 0.0 A 0 W 0.00
5 Branch 7 0.2 A 11 W 0.29
6 Branch 8 0.1 A 8 W 0.25
7 Branch 9 0.1 A 10 W 0.30
8 Branch 10 0.3 A 0 W 0.00
9 Branch 11 0.2 A 0 W 0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified branch circuit pole.
disable	Disables the upper warning threshold for the specified branch circuit pole.
A numeric value	Sets a value for the upper warning threshold of the specified branch circuit pole and enables this threshold at the same time.

Example

The following command sets the Upper Warning threshold for the pole 2 (L2) current of the branch circuit #4 to 10A, and simultaneously enables the upper warning threshold if this threshold has not been enabled yet.

```
config:#   sensor branchpole 4 L2 current upperWarning 10
```

Setting the Lower Critical Threshold for a Branch Circuit Pole

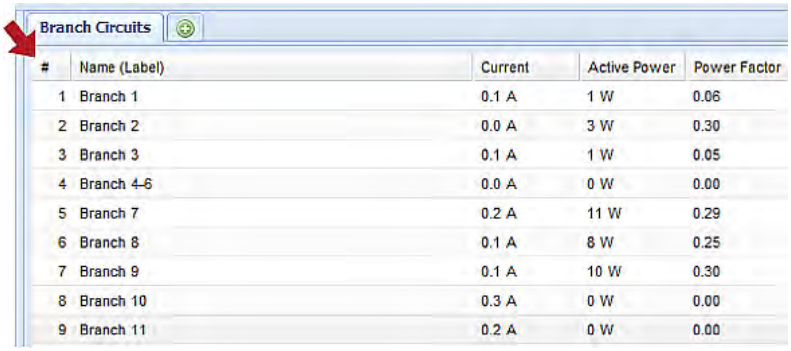
This command syntax configures the Lower Critical threshold of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified branch circuit pole.
disable	Disables the lower critical threshold for the specified branch circuit pole.
A numeric value	Sets a value for the lower critical threshold of the specified branch circuit pole and enables this threshold at the same time.

Example

The following command enables the Lower Critical threshold for the pole 2 (L2-L3) voltage of the branch circuit #4.

```
config:#   sensor branchpole 4 L2 voltage lowerCritical enable
```

Setting the Lower Warning Threshold for a Branch Circuit Pole

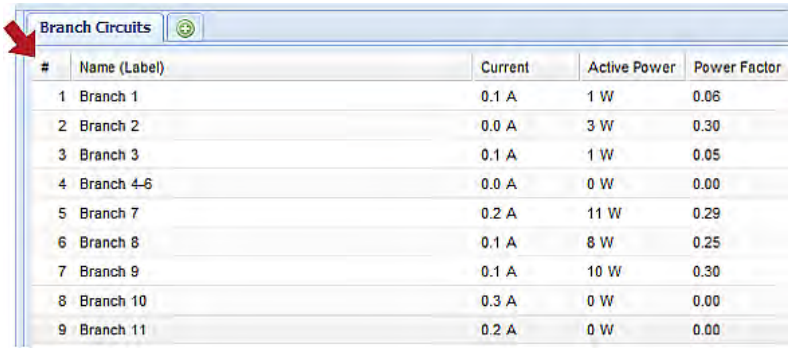
This command syntax configures the Lower Warning threshold of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified branch circuit pole.
disable	Disables the lower warning threshold for the specified branch circuit pole.
A numeric value	Sets a value for the lower warning threshold of the specified branch circuit pole and enables this threshold at the same time.

Example

The following command sets the Lower Warning threshold for the pole 3 (L3) current of the branch circuit #4 to 5A, and simultaneously enables the lower warning threshold if this threshold has not been enabled yet.

```
config:#   sensor branchpole 4 L3 current lowerWarning 5
```

Setting the Branch Circuit Pole's Deassertion Hysteresis

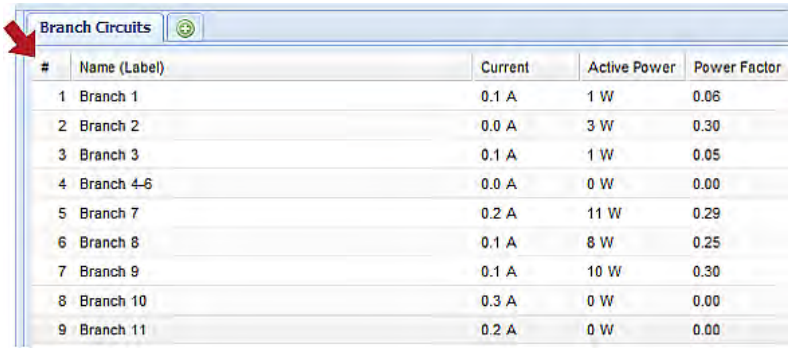
This command syntax configures the deassertion hysteresis value of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> hysteresis <value>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.


Branch Circuits
Name (Label) Current Active Power Power Factor
1 Branch 1 0.1 A 1 W 0.06
2 Branch 2 0.0 A 3 W 0.30
3 Branch 3 0.1 A 1 W 0.05
4 Branch 4-6 0.0 A 0 W 0.00
5 Branch 7 0.2 A 11 W 0.29
6 Branch 8 0.1 A 8 W 0.25
7 Branch 9 0.1 A 10 W 0.30
8 Branch 10 0.3 A 0 W 0.00
9 Branch 11 0.2 A 0 W 0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified branch circuit pole. See ***What is Deassertion Hysteresis?*** (on page 86) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the pole 2 (L2) current of the branch circuit #4 to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor branchpole 4 L2 current hysteresis 0.2
```

Setting the Branch Circuit Pole's Assertion Timeout

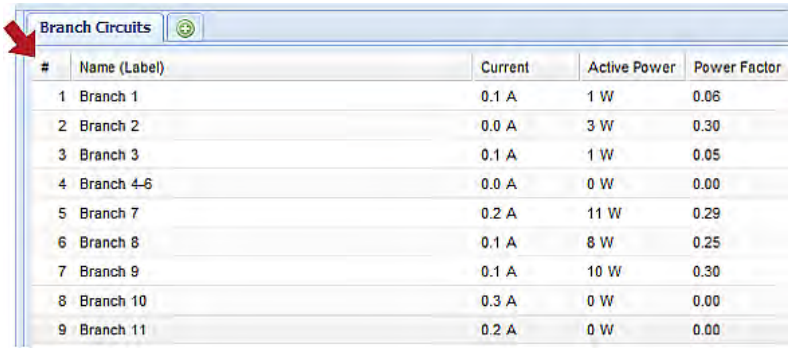
This command syntax configures the assertion timeout value of a branch circuit pole.

```
config:#   sensor branchpole <n> <p> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the index number of the desired branch circuit channel.

  This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the Branch Circuit Monitor.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- <p> is the label of the branch circuit pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified branch circuit pole. See ***What is Assertion Timeout?*** (on page 88).

Example

The following command sets the assertion timeout value of the pole 2 (L2) current of the branch circuit #7 to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor branchpole 7 L2 current assertionTimeout 4
```

Commands for Mains Sensors

A sensor configuration command for the mains begins with *sensor mains*.

Setting the Mains Channels' Upper Critical Threshold

This command syntax configures the Upper Critical threshold of the mains channels.

```
config:#   sensor mains <sensor type> upperCritical <option>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the mains channels.
disable	Disables the upper critical threshold for the mains channels.
A numeric value	Sets a value for the upper critical threshold of the mains channel and enables this threshold at the same time.

Example

The following command enables the Upper Critical threshold for the mains channels' RMS current.

```
config:#   sensor mains current upperCritical enable
```

Setting the Mains Channels' Upper Warning Threshold

This command syntax configures the Upper Warning threshold of the mains channels.

```
config:#   sensor mains <sensor type> upperWarning <option>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the mains channels.
disable	Disables the upper warning threshold for the mains channels.
A numeric value	Sets a value for the upper warning threshold of the mains channels and enables this threshold at the same time.

Example

The following command sets the Upper Warning threshold for the mains channels' RMS current to 60A. It also enables the upper warning threshold if this threshold has not been enabled yet.

```
config:#   sensor mains current upperWarning 60
```

Setting the Mains Channels' Lower Critical Threshold

This command syntax configures the Lower Critical threshold of the mains channels.

```
config:#   sensor mains <sensor type> lowerCritical <option>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the mains channels.
disable	Disables the lower critical threshold for the mains channels.
A numeric value	Sets a value for the lower critical threshold of the mains channels and enables this threshold at the same time.

Example

The following command disables the Lower Critical threshold for the mains channels' current.

```
config:#   sensor mains current lowerCritical disable
```

Setting the Mains Channels' Lower Warning Threshold

This command syntax configures the Lower Warning threshold of the mains channels.

```
config:#   sensor mains <sensor type> lowerWarning <option>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the mains channels.
disable	Disables the lower warning threshold for the mains channels.
A numeric value	Sets a value for the lower warning threshold of the mains channels and enables this threshold at the same time.

Example

The following command sets the Lower Warning threshold for the mains channels' current to 50A, and simultaneously enables the lower warning threshold if this threshold has not been enabled yet.

```
config:#   sensor mains current lowerWarning 50
```

Setting the Mains Channels' Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of the mains channel.

```
config:#   sensor mains <sensor type> hysteresis <value>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the mains channels. See ***What is Deassertion Hysteresis?*** (on page 86) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis for the mains channels' RMS current to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor mains current hysteresis 0.2
```

Setting the Mains Channels' Assertion Timeout

This command syntax configures the assertion timeout value of the mains channels.

```
config:#   sensor mains <sensor type> assertionTimeout <value>
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the mains channels. See ***What is Assertion Timeout?*** (on page 88).

Example

The following command sets the assertion timeout value of the mains channels' RMS current to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor mains current assertionTimeout 4
```

Commands for Mains Pole Sensors

A sensor configuration command for mains poles begins with *sensor mainspole*.

Setting the Upper Critical Threshold for a Mains Pole

This command syntax configures the Upper Critical threshold of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> upperCritical <option>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified mains pole.
disable	Disables the upper critical threshold for the specified mains pole.
A numeric value	Sets a value for the upper critical threshold of the specified mains pole and enables this threshold at the same time.

Example

The following command disables the Upper Critical threshold for the pole 3 (L3-L1) voltage of the mains channels.

```
config:#   sensor mainspole L3 voltage upperCritical disable
```

Setting the Upper Warning Threshold for an Inlet Pole

This command syntax configures the Upper Warning threshold of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> upperWarning <option>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified mains pole.

Option	Description
disable	Disables the upper warning threshold for the specified mains pole.
A numeric value	Sets a value for the upper warning threshold of the specified mains pole and enables this threshold at the same time.

Example

The following command sets the Upper Warning threshold for the pole 2 (L2-L3) voltage of the mains channels to 427V, and simultaneously enables the upper warning threshold if this threshold has not been enabled yet.

```
config:#   sensor mainspole L2 voltage upperWarning 427
```

Setting the Lower Critical Threshold for an Inlet Pole

This command syntax configures the Lower Critical threshold of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> lowerCritical <option>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor

Sensor type	Description
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified mains pole.
disable	Disables the lower critical threshold for the specified mains pole.
A numeric value	Sets a value for the lower critical threshold of the specified mains pole and enables this threshold at the same time.

Example

The following command enables the Lower Critical threshold for the pole 2 (L2-L3) voltage of the mains channnels.

```
config:#   sensor mainspole L2 voltage lowerCritical enable
```

Setting the Lower Warning Threshold for a Mains Pole

This command syntax configures the Lower Warning threshold of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> lowerWarning <option>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified mains pole.
disable	Disables the lower warning threshold for the specified mains pole.
A numeric value	Sets a value for the lower warning threshold of the specified mains pole and enables this threshold at the same time.

Example

The following command sets the Lower Warning threshold for the pole 3 (L3-L1) voltage of the mains channels to 184V, and simultaneously enables the lower warning threshold if this threshold has not been enabled yet.

```
config:#   sensor mainspole L3 voltage lowerWarning 184
```

Setting the Mains Pole's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> hysteresis <value>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified mains pole. See ***What is Deassertion Hysteresis?*** (on page 86) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the pole 2 (L2) current of the mains channels to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor mainspole L2 current hysteresis 0.2
```

Setting the Mains Pole's Assertion Timeout

This command syntax configures the assertion timeout value of a mains pole.

```
config:#   sensor mainspole <p> <sensor type> assertionTimeout <value>
```

Variables:

- <p> is the label of the mains pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified mains pole. See ***What is Assertion Timeout?*** (on page 88).

Example

The following command sets the assertion timeout value of the pole 2 (L2) current of the mains channels to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor mainspole L2 current assertionTimeout 4
```

Commands for Environmental Sensors

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

Setting the Sensor's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified environmental sensor.
disable	Disables the upper critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Setting the Sensor's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified environmental sensor.
disable	Disables the upper warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold of the environmental "temperature" sensor with the ID number 4.

```
config:#   sensor externalsensor 4 temperature upperWarning enable
```

Setting the Sensor's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified environmental sensor.
disable	Disables the lower critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold of the environmental "humidity" sensor with the ID number 1 to 15%. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Setting the Sensor's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified environmental sensor.
disable	Disables the lower warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command disables the Lower Warning threshold of the environmental "humidity" sensor with the ID number 3.

```
config:#   sensor externalsensor 3 humidity lowerWarning disable
```

Setting the Sensor's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***What is Deassertion Hysteresis?*** (on page 86) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the environmental "temperature" sensor with the ID number 4 to 2 degrees Celsius. That is, the temperature must drop by at least 2 degrees Celsius below the upper threshold or rise by at least 2 degrees Celsius above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Setting the Sensor's Assertion Timeout

This command syntax configures the assertion timeout value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the Branch Circuit Monitor web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. See ***What is Assertion Timeout?*** (on page 88).

Example

The following command sets the assertion timeout of the environmental "temperature" sensor with the ID number 3 to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor externalsensor 3 temperature assertionTimeout 4
```

User Configuration Commands

Most of user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command syntax creates a new user profile.

```
config:#   user create <name> <option> <roles>
```

After performing the user creation command, the Branch Circuit Monitor prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 289).*

Changing a User's Password

This command syntax allows you to change an existing user's password if you have the Administrator Privileges.

```
config:#   user modify <name> password
```

After performing the above command, Branch Circuit Monitor prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

Variables:

- <name> is the name of the user whose settings you want to change.

Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 181).
2. Type the following command to change the password for the user profile "May."

   ```
   config:#   user modify May password
   ```
3. Type a new password when prompted, and press Enter.
4. Type the same new password and press Enter.
5. If the password change is completed successfully, the config:# prompt appears.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

- **To change a user's full name, use this command syntax:**

```
config:#   user modify <name> fullName "<full_name>"
```

- **To change a user's telephone number, use this command syntax:**

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

- **To change a user's email address, use this command syntax:**

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command modifies two parameters for the user profile -- May:

```
config:#   user modify May fullName "May Turner" telephoneNumber 123-4567
```

Results:

- May's full name is specified as May Turner.
- May's telephone number is set to 123-4567.

Enabling or Disabling a User Profile

This command syntax enables or disables a user profile. A user can log in to the Branch Circuit Monitor device only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Example

The following command enables the user profile -- May.

```
config:#   user modify May enabled true
```

Forcing a Password Change

This command syntax determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#   user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Example

The following command enforces a password change on May's next login.

```
config:#   user modify May forcePasswordChangeOnNextLogin true
```

Modifying the SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See ***Multi-Command Syntax*** (on page 289).

To enable or disable the SNMP v3 access to Branch Circuit Monitor for the specified user:

```
config:#   user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

To determine the security level:

```
config:#   user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

To determine whether the authentication passphrase is identical to the password:

```
config:#    user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

To determine the authentication passphrase:

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising up to 32 ASCII printable characters.

To determine whether the privacy passphrase is identical to the authentication passphrase:

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.

Option	Description
false	Privacy passphrase is different from the authentication passphrase.

To determine the privacy passphrase:

```
config:#   user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising up to 32 ASCII printable characters.

To determine the authentication protocol:

```
config:#   user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

To determine the privacy protocol:

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.

Option	Description
AES-128	AES-128 privacy protocol is applied.

Example

The following command sets three SNMPv3 prameters of the user "May."

```
config:#   user modify May snmpV3Access enable securityLevel authNoPriv
           userPasswordAsAuthenticationPassPhrase true
```

Results:

- The user's SNMPv3 access permission is enabled.
- The SNMPv3 security level is authentication only, no privacy.
- The authentication passphrase is identical to the user's password.

Changing the Role(s)

This command syntax changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command assigns two roles to the user "May."

```
config:#   user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Changing the Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time. To combine all commands, see ***Multi-Command Syntax*** (on page 289).

Note: The measurement unit change only applies to the web interface and command line interface.

To set the preferred temperature unit:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

To set the preferred length unit:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

To set the preferred pressure unit:

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Example

The following command sets all measurement unit preferences for the user "May."

```
config:#   user modify May preferredTemperatureUnit F preferredLengthUnit feet
           preferredPressureUnit psi
```

Results:

- The preferred temperature unit is set to Fahrenheit.
- The preferred length unit is set to feet.
- The preferred pressure unit is set to psi.

Deleting a User Profile

This command syntax deletes an existing user profile.

```
config:#   user delete <name>
```

Example

The following command deletes the user profile "May."

```
config:#   user delete May
```

Changing Your Own Password

Every user can change their own password via this command syntax if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:#    password
```

After performing this command, the Branch Circuit Monitor prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Example

This procedure changes your own password:

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 181).
2. Type the following command and press Enter.

   ```
   config:#    password
   ```

3. Type the existing password and press Enter when the following prompt appears.

   ```
   Current password:
   ```

4. Type the new password and press Enter when the following prompt appears.

   ```
   Enter new password:
   ```

5. Re-type the new password for confirmation and press Enter when the following prompt appears.

   ```
   Re-type new password:
   ```

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command syntax creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 282).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

All Privileges

This table lists all privileges.

Privilege	Description
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeEventSetup	Change Event Settings
changeExternalSensorsConfiguration	Change External Sensors Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings

Privilege	Description
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
viewEventSetup	View Event Settings
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Images and Configuration

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

Example

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

To modify a role's description:

```
config:#   role modify <name> description <description>
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

To add more privileges to a specific role:

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> addPrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 282).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

To remove specific privileges from a role:

```
config:#   role modify <name> removePrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 282).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

Example

The following command modifies the privileges of the role "tester."

```
config:#   role modify tester addPrivileges changeAuthSettings removePrivileges
           firmwareUpgrade
```

Results:

- The "changeAuthSettings" (Change Authentication Settings) privilege is added to the role.
- The "firmwareUpgrade" (Firmware Upgrade) privilege is removed from the role.

Deleting a Role

This command syntax deletes an existing role.

```
config:#   role delete <name>
```

Example

The following command deletes an existing role.

```
config:#   role delete tester
```

EnergyWise Configuration Commands

An EnergyWise configuration command begins with *energywise*.

Enabling or Disabling EnergyWise

This command syntax determines whether the Cisco® EnergyWise endpoint implemented on the Branch Circuit Monitor device is enabled.

```
config:#   energywise enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

Example

The following command enables the Cisco® EnergyWise feature.

```
config:#   energywise enabled true
```

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the Branch Circuit Monitor device belongs.

```
config:#   energywise domain <name>
```

Variables:

- <name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Example

The following command configures the Branch Circuit Monitor device to belong to the Cisco® EnergyWise domain named "helloDomain."

```
config:#   energywise domain helloDomain
```

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco® EnergyWise domain.

```
config:#   energywise secret <password>
```

Variables:

- <password> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Example

The following command specifies "password5233" as the Cisco® EnergyWise domain secret (password).

```
config:#   energywise secret password5233
```

Changing the UDP Port

This command syntax specifies the UDP port for communications in the Cisco® EnergyWise domain.

```
config:#   energywise port <port>
```

Variables:

- <port> is the UDP port number ranging between 1 and 65535.

Example

The following command specifies 10288 as the UDP port for Cisco® EnergyWise.

```
config:#   energywise port 10288
```

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the Branch Circuit Monitor device.

```
config:#   energywise polling <timing>
```

Variables:

- <timing> is an integer number in seconds. It ranges between 30 and 600 seconds.

Example

The following command determines the polling interval to query the Branch Circuit Monitor device is 300 seconds.

```
config:#   energywise polling 300
```

Setting the History Buffer Length

This command syntax changes the history buffer length. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.
- If you leave the <n> variable blank when using the command, the history buffer is set to 25 by default.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command and perform all of them at a time.

A multi-command syntax looks like this:

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask
           255.255.255.0 gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 3rd circuit breaker.

```
config:#   sensor ocp 3 current upperCritical disable upperWarning 20
```

Results:

- The Upper Critical threshold of the 3rd circuit breaker's RMS current is disabled.
- The Upper Warning threshold of the 3rd circuit breaker's RMS current is set to 20A and enabled at the same time.

Example 3 - Combination of SSID and PSK Parameters

This multi-command syntax configures both of SSID and PSK parameters simultaneously for the wireless feature.

```
config:#   network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Quitting the Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

To quit the configuration mode, use either command:

```
config:#    apply
```

-- OR --

```
config:#    cancel
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Unblocking a User

If any user is blocked from accessing the Branch Circuit Monitor, you can unblock them at the local console.

To unblock a user:

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 162).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the login name of the user to be unblocked and press Enter.

```
Username to unblock:
```

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the Branch Circuit Monitor

You can reset the Branch Circuit Monitor device to factory defaults or simply restart it using the CLI commands.

Restarting the Device

This command restarts the Branch Circuit Monitor device. It is not a factory default reset.

To restart the Branch Circuit Monitor device:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the Branch Circuit Monitor device.

```
#     reset unit
```

-- OR --

```
#     reset unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Resetting to Factory Defaults

This command restores all settings of the Branch Circuit Monitor device to factory defaults.

▶ **To reset Branch Circuit Monitor settings, use either command:**

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

See ***Using the CLI Command*** (on page 305) for more information.

Network Troubleshooting

The Branch Circuit Monitor provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering the Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

▶ **To enter the diagnostic mode:**

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `diag` and press Enter. The diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying the DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>       nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Example

The following command checks the DNS information regarding the host 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Showing the Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Example

The following command displays the server connections to your Branch Circuit Monitor device.

```
diag>       netstat connections
```

Testing the Network Connectivity

This command syntax sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good, or the host is shut down or not being connected to the network.

```
diag>       ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number.
size <number2>	Determines the packet size. <number2> is an integer number in bytes.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds.

The command looks like this syntax when it includes all options:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Example

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping 192.168.84.222 count 5
```

Tracing the Route

This command syntax traces the network route between your Branch Circuit Monitor device and a network host.

```
diag>       traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example

The following command displays the existing network routing for the host 192.168.84.222.

```
diag>       traceroute 192.168.84.222
```

Quitting the Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command, you can have the CLI show them by adding a space and then a question mark to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

- **To query available parameters for the "show" command, the syntax is:**

```
#           show ?
```

- **To query available network configuration parameters, the syntax is:**

```
config:#    network ?
```

- **To query available role configuration parameters, the syntax is:**

```
config:#    role ?
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. For some *unique* CLI commands, such as the "reset" command, you can easily complete them by pressing the Tab or Ctrl+i instead of typing the whole command word by word.

- **To have a unique command completed automatically:**

1. Type initial letters or words of the command. For example, type the first word of the "`reset factorydefaults`" command, that is, `reset`.
2. Press Tab or Ctrl+i until the complete command appears. For example, although you typed only one word for the reset command, the rest of the command appears after pressing Tab or Ctrl+i.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Appendix A Specifications

In This Chapter

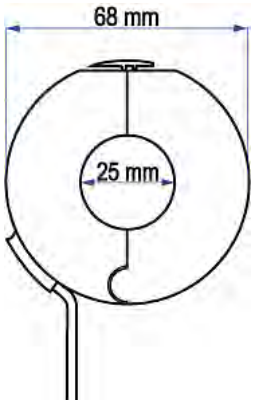
Branch Circuit Monitor Specifications.....298
CT Specifications.....298
Power Measurement Accuracy 300
Maximum Ambient Operating Temperature 301
Serial RS-232 Port Pinouts.....301
Sensor RJ-12 Port Pinouts.....302

Branch Circuit Monitor Specifications

Model	Maximum circuits (lines)	Input power	Frequency	Update rate
BCM-2400	24 circuits, including 21 branch circuits rated up to 30A and 1 three-phase mains rated up to 200A	Three-phase wye-connected, 190-415VAC, 20A (North America) or 16A (Europe)	50/60 Hz	1 second

CT Specifications

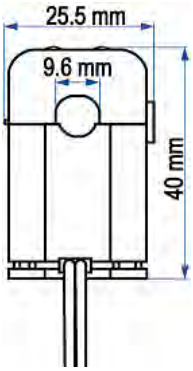
Raritan Mains CT



Mains CT electric specifications	
Rated primary current (RMS) 50/60Hz	200A (1-250A)
Maximum current (continuous)	360A

Mains CT electric specifications	
Turns ratio	Np:Ns=1:3000
Secondary output at rated current	333mV (resistor inside the CT)
D.C. resistance maximum at 20 degrees Celsius	120 ohm
Accuracy	1%
Linearity	0.5%
Phase error at rated current range	smaller than or equal to 1 degree
Operating temperature	-40 to 85 degrees Celsius
Storage temperature	-45 to 90 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2.5KV/1mA/1min
Impulse withstand voltage	5KV peak
Insulation resistance	DC500V/100M ohm min

Raritan Branch Circuit CT



Branch Circuit CT electric specifications	
Rated primary current 50/60Hz	30A (1-60A)
Current ratio	30A/15mA
Turns ratio	Np:Ns=1:2000
Winding D.C. resistance maximum at 20 degrees Celsius	250 ohm

Branch Circuit CT electric specifications	
Accuracy @RL< or = 10 ohm	2%
Operating temperature	-40 to 65 degrees Celsius
Storage temperature	-45 to 85 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2500V/1mA/1min
Impulse withstand voltage	5KV peak
Insulation resistance	DC500V/100M ohm min

Power Measurement Accuracy

The following measurement accuracy applies to all Raritan Branch Circuit Monitor models and CTs.

Mains Accuracy

The following data applies only to Raritan's mains CTs and the mains channels on the Branch Circuit Monitor.

	Mains CT's measurement accuracy	Mains measurement accuracy
RMS voltage (V)		2%
RMS current (A)	1%	2%
Active power (Watts)		2%
Apparent power (VA)		2%
Active energy (Watts-hour)		2%

Branch Circuit Accuracy

The following data applies only to Raritan's branch circuit CTs and the branch circuit channels on the Branch Circuit Monitor.

	Branch circuit CT's measurement accuracy	Branch circuit measurement accuracy
RMS voltage (V)		2%
RMS current (A)	2%	3%
Active power (Watts)		3%
Apparent power (VA)		3%
Active energy (Watts-hour)		3%

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for all Branch Circuit Monitor models are the same.

Specification	Measure
Max Ambient Temperature	50 degrees Celsius

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready

RS-232 Pin/signal definition			
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

Appendix B Circuit Monitoring Worksheet

Branch Circuit Monitor Model _____

Branch Circuit Monitor Serial Number _____

Electrical Panel _____

1 (CT number)	(Circuit name)	**2** (CT number)	(Circuit name)
3 (CT number)	(Circuit name)	**4** (CT number)	(Circuit name)
5 (CT number)	(Circuit name)	**6** (CT number)	(Circuit name)
7 (CT number)	(Circuit name)	**8** (CT number)	(Circuit name)
9 (CT number)	(Circuit name)	**10** (CT number)	(Circuit name)
11 (CT number)	(Circuit name)	**12** (CT number)	(Circuit name)
13 (CT number)	(Circuit name)	**14** (CT number)	(Circuit name)
15 (CT number)	(Circuit name)	**16** (CT number)	(Circuit name)
17 (CT number)	(Circuit name)	**18** (CT number)	(Circuit name)
19 (CT number)	(Circuit name)	**20** (CT number)	(Circuit name)
21 (CT number)	(Circuit name)		

Appendix C Resetting to Factory Defaults

For security reasons, the Branch Circuit Monitor device can be reset to factory defaults only at the local console.

Important: Exercise caution before resetting the Branch Circuit Monitor to its factory defaults. This erases existing information and customized settings, such as user profiles and threshold values. Only active energy data and firmware upgrade history are retained forever.

You can use either the reset button or the command line interface (CLI) to reset the Branch Circuit Monitor.

In This Chapter

Using the Reset Button.....304
Using the CLI Command 305

Using the Reset Button

This section describes how to reset the Branch Circuit Monitor device via the reset button.

To reset to factory defaults using the reset button:

1. Connect a computer to the Branch Circuit Monitor device. See ***Connecting the Branch Circuit Monitor to a Computer*** (on page 15).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Branch Circuit Monitor. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 18).
3. Press (and release) the Reset button of the Branch Circuit Monitor device while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the Branch Circuit Monitor to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the Branch Circuit Monitor to factory defaults. For information on CLI, see ***Using the Command Line Interface*** (on page 161).

To reset to factory defaults using the CLI command:

1. Connect a computer to the Branch Circuit Monitor device. See ***Connecting the Branch Circuit Monitor to a Computer*** (on page 15).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Branch Circuit Monitor. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 18).
3. Log in to the CLI by typing the user name "admin" and its password. See Step 4 of ***Initial Network Configuration*** (on page 18).
4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #     reset factorydefaults
   ```

   -- OR --

   ```
   #     reset factorydefaults /y
   ```

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.
6. Wait until the Username prompt appears, indicating the reset is complete.

Appendix D LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and groups intended for the Branch Circuit Monitor

b. Create user groups for the Branch Circuit Monitor on the AD server

c. Configure LDAP authentication on the Branch Circuit Monitor device

d. Configure roles on the Branch Circuit Monitor device

In This Chapter

Step A. Determine User Accounts and Groups 306
Step B. Configure User Groups on the AD Server 307
Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device 308
Step D. Configure Roles on the Branch Circuit Monitor 311

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing the Branch Circuit Monitor. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

User groups	User accounts (members)
BCM_User	usera
	bcmuser2
BCM_Admin	userb
	bcmuser

Group permissions:

- The BCM_User group will only have read-only permissions.
- The BCM_Admin group will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups for the Branch Circuit Monitor on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

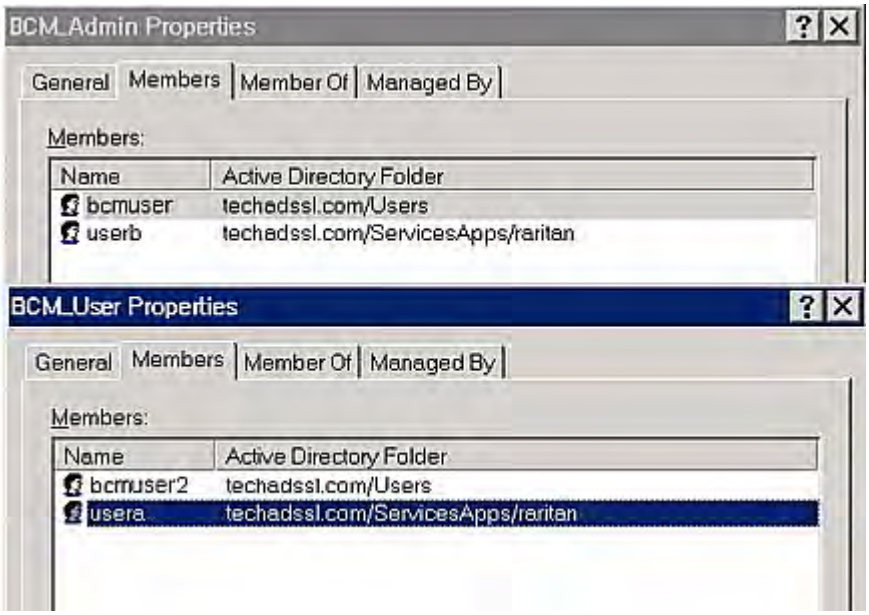
- The groups for the Branch Circuit Monitor are named *BCM_Admin* and *BCM_User*.
- User accounts *bcmuser*, *bcmuser2*, *usera* and *userb* already exist on the AD server.

To configure the user groups on the AD server:

1. On the AD server, create new groups -- *BCM_Admin* and *BCM_User*.

   Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *bcmuser2* and *usera* accounts to the BCM_User group.
3. Add the *bcmuser* and *userb* accounts to the BCM_Admin group.
4. Verify whether each group comprises correct users.



Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device

You must enable and set up LDAP authentication properly on the Branch Circuit Monitor device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying the Network Settings*** (on page 62) and ***Role of a DNS Server*** (on page 66).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over SSL.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

To configure LDAP authentication:

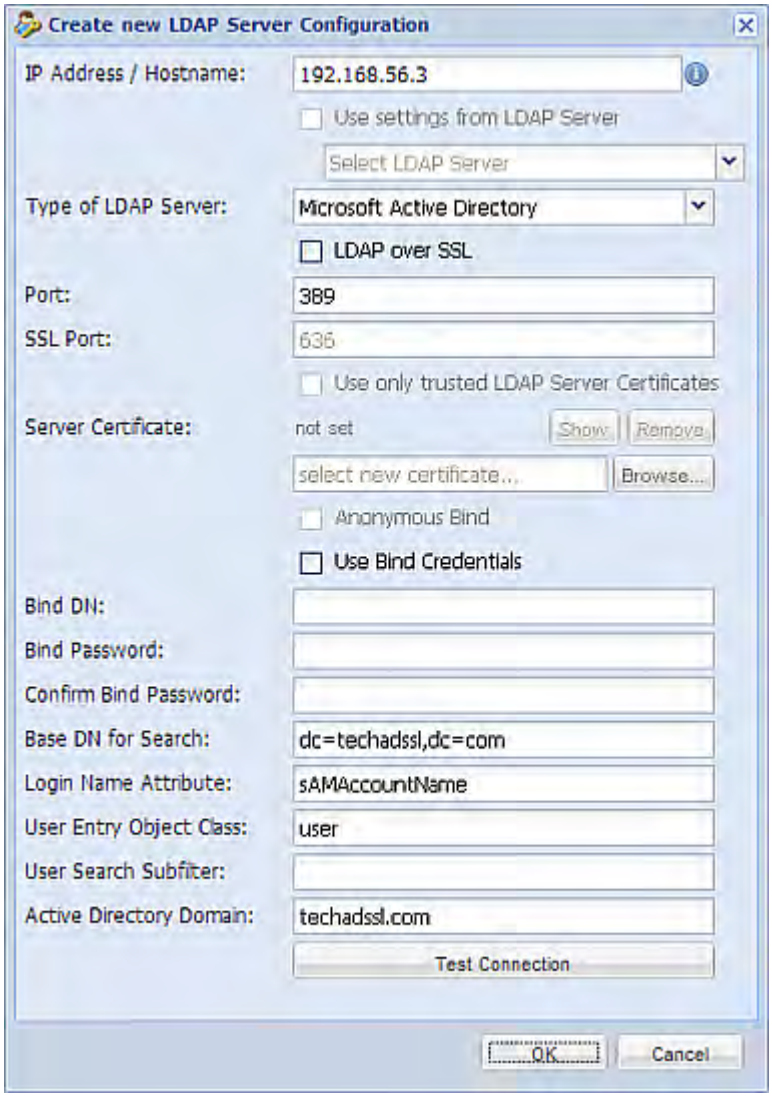
1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the Branch Circuit Monitor with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - LDAP over SSL - Have the checkbox deselected since the SSL encryption is not applied in this example.
   - Port - Ensure the field is set to 389.
   - SSL Port and Server Certificate - Skip the two fields since the SSL encryption is not enabled.
   - Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.

- Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.
- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.

- Active Directory Domain - Type `techadssl.com`.



Note: For more information on LDAP configuration, see **Setting Up LDAP Authentication** *(on page 112).*

5. Click OK to save the changes. The LDAP server is saved.
6. Click OK to save the changes. The LDAP authentication is activated.

Note: If the Branch Circuit Monitor clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the Branch Circuit Monitor and the LDAP server to use the same NTP server.

Step D. Configure Roles on the Branch Circuit Monitor

A role on the Branch Circuit Monitor determines the system permissions. You must create the roles whose names are identical to the user groups created for the Branch Circuit Monitor on the AD server or authorization will fail. Therefore, we will create the roles named *BCM_User* and *BCM_Admin* on the Branch Circuit Monitor.

In this illustration, we assume:

- Users assigned to the *BCM_User* role can only access the Branch Circuit Monitor and view settings.
- Users assigned to the *BCM_Admin* role can both access and configure the Branch Circuit Monitor because they have the Administrator permissions.

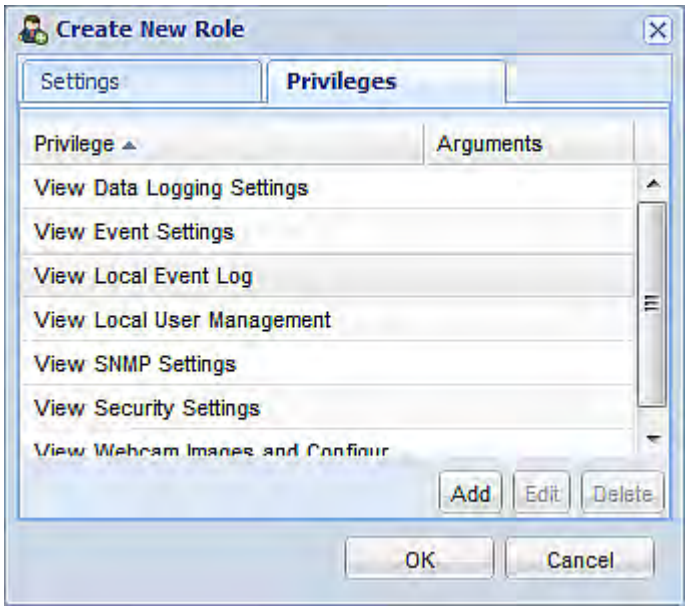
To create the BCM_User role with appropriate permissions assigned:

1. Choose User Management > Roles. The Manage Roles dialog appears.

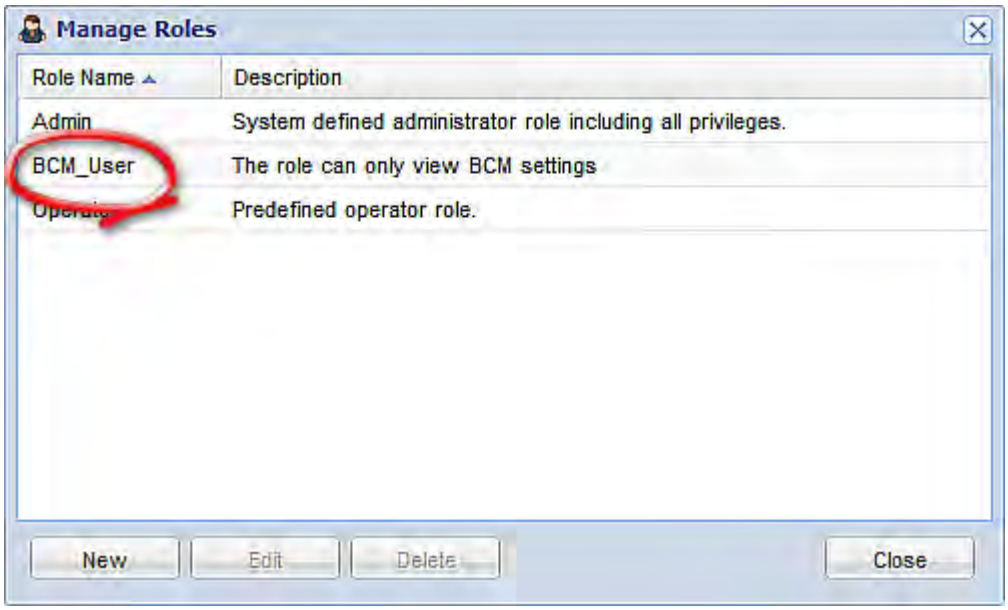
   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `BCM_User` in the Role Name field.
4. Type a description for the BCM_User role in the Description field. In this example, we type "The role can only view BCM settings" to describe the role.
5. Click the Privileges tab to select all View XXX permissions (where XXX is the name of the setting). A View XXX permission lets users view the XXX settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select a permission beginning with the word "View" from the Privileges list, such as View Event Settings.
   c. Click Add.

d. Repeat Steps a to c to add all permissions beginning with "View."



6. Click OK to save the changes. The BCM_User role is created.

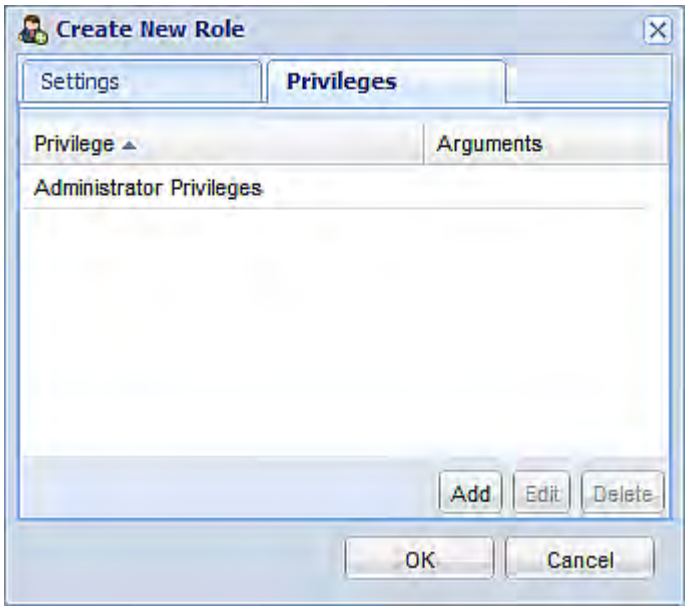


7. Keep the Manage Roles dialog opened to continue creating the BCM_Admin role.

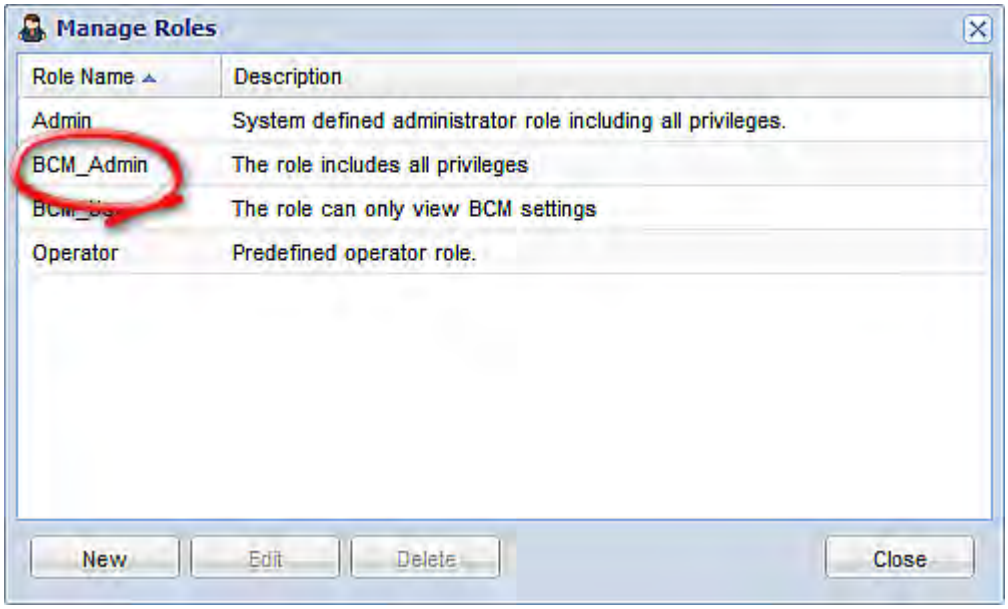
To create the BCM_Admin role with full permissions assigned:

1. Click New. The Create New Role dialog appears.

2. Type `BCM_Admin` in the Role Name field.
3. Type a description for the BCM_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all Branch Circuit Monitor settings.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission named Administrator Privileges from the Privileges list.
   c. Click Add.



5. Click OK to save the changes. The BCM_Admin role is created.



6. Click Close to quit the dialog.

Appendix E Additional Branch Circuit Monitor Information

In This Chapter

Altitude Correction Factors 315
RF Code Energy Monitoring Solution 316

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

RF Code Energy Monitoring Solution

With the RF Code active RFID hardware and management software and Raritan's Branch Circuit Monitor combined, a wire-free energy monitoring solution that provides a picture of power utilization is offered.

This combined solution does not require any additional IP address configuration or association. All you need to do is plug an RF Code R170 PDU sensor tag into the SENSOR port of the Branch Circuit Monitor device.

The RF Code R170 PDU sensor tag collects the power data generated by Raritan Branch Circuit Monitor and sends the data to the RF Code Sensor Manager software, which not only manages the power data but also make computations about the power usage from the collected data.

You can use the RF Code Sensor Manager to manage the power data using:

- Live table views
- Map views
- Interactive graphing and reporting
- Scheduled graphing and reporting
- Alerting and thresholding

Index

A

A Note about Enabling Thresholds • 160
A Note about Untriggered Rules • 128
About Contact Closure Sensors • 28
About the Interface • 161
Access Security Control • 95
Accessing the Help • 153
Add Page Icon • 49, 52
Adding a Firewall Rule • 209, 211
Adding a Role-Based Access Control Rule • 224
Adding IT Devices for Ping Monitoring • 131
Adding the LDAP Server Settings • 113
Additional Branch Circuit Monitor Information • 315
Adjusting the Pane • 51
All Privileges • 282, 285
Altitude Correction Factors • 72, 183, 315
Automatically Completing a Command • 296

B

Before You Begin • 4
Branch Circuit Accuracy • 301
Branch Circuit Channel Configuration Commands • 227
Branch Circuit Channels • 35
Branch Circuit Information • 39, 168
Branch Circuit Monitor Specifications • 298
Branch Circuit Pole Threshold Information • 172
Branch Circuit Threshold Information • 171
Browser-Defined Shortcut Menu • 57
Browsing through the Online Help • 153
Bulk Configuration for Branch Circuit Thresholds • 84, 85

C

Certificate Signing Request • 108
Changing a User's Password • 272
Changing the Branch Circuit Channel Name • 227
Changing the Column • 56
Changing the Default Policy • 96, 97, 104
Changing the Device Name • 181
Changing the HTTP Port • 202
Changing the HTTP(S) Settings • 66
Changing the HTTPS Port • 202
Changing the Inlet Name • 228
Changing the LAN Duplex Mode • 201
Changing the LAN Interface Speed • 200
Changing the Measurement Units • 72, 145, 279
Changing the Role List View • 95
Changing the Role(s) • 278
Changing the Sensor Description • 232
Changing the Sensor Name • 229
Changing the Sorting • 56, 130, 133
Changing the SSH Configuration • 203
Changing the SSH Port • 204
Changing the SSH Settings • 67, 90
Changing the Telnet Configuration • 202
Changing the Telnet Port • 203
Changing the Telnet Settings • 67
Changing the UDP Port • 288
Changing the User List View • 92
Changing the View of a List • 55, 60, 92, 95, 129, 149, 152
Changing Your Own Password • 281
Changing Your Password • 45
Channel Convention • 6, 10, 13, 34, 78
Channel Management • 76
Channels • 34
Checking Server Monitoring States • 132
Checking the AC Electrical Panel • 5
Circuit Monitoring Worksheet • 5, 8, 303
Clearing Event Entries • 129
Closing a Serial Connection • 164
Collapsing the Tree • 50
Command History • 179
Commands for Branch Circuit Pole Sensors • 242
Commands for Branch Circuit Sensors • 233
Commands for Environmental Sensors • 265
Commands for Mains Pole Sensors • 257
Commands for Mains Sensors • 251
Components of an Event Rule • 119
Configuring a Contact Closure Sensor • 29, 30, 141
Configuring Environmental Sensors • 133, 136
Configuring Event Rules • 68, 74, 83, 118, 121, 157
Configuring IP Protocol Settings • 185
Configuring SNMP Traps • 157

Configuring the Branch Circuit Channels • 24, 77, 79, 172, 242
Configuring the Branch Circuit Monitor • 14, 62
Configuring the Branch Circuit Monitor Device and Network • 180
Configuring the Firewall • 96
Configuring the IPv4 Parameters • 193
Configuring the IPv6 Parameters • 197
Configuring the Mains Channels • 76
Configuring the SMTP Settings • 74, 120
Configuring the SNMP Settings • 68, 89
Configuring Users for Encrypted SNMP v3 • 68, 156
Connecting a Logitech Webcam (Optional) • 32, 49, 50, 147
Connecting Branch Circuit CTs • 8, 12, 35
Connecting Environmental Sensors (Optional) • 26, 133
Connecting Mains CTs • 7, 9, 35
Connecting the Branch Circuit Monitor to a Computer • 15, 304, 305
Connecting the Branch Circuit Monitor to Your Network • 17, 60, 61
Connecting Third-Party Detectors/Switches to DPX-CC2-TR • 28
Connection Ports • 35
Contact Closure Sensor LEDs • 30
Control Buttons • 38
Copying a Branch Circuit Monitor Configuration • 145
Copying Configurations with Bulk Configuration • 143
Creating a Certificate Signing Request • 108
Creating a Role • 91, 93, 281
Creating a Self-Signed Certificate • 110
Creating a User Profile • 44, 67, 88, 92, 93, 94, 146, 156, 270
Creating Actions • 119
Creating an Event Rule • 119
Creating Firewall Rules • 96, 98
Creating Role-Based Access Control Rules • 104, 105
Creating Rules • 121
CT Dimensions • 9
CT Specifications • 76, 77, 298
CT Terminals and Buttons • 35

D

Data Pane • 53
Deleting a Firewall Rule • 214
Deleting a Role • 95, 286
Deleting a Role-Based Access Control Rule • 227
Deleting a User Profile • 92, 280
Deleting an Event Rule or Action • 128
Deleting Firewall Rules • 100
Deleting Ping Monitoring Settings • 132
Deleting Role-Based Access Control Rules • 107
Deleting the LDAP Server Settings • 117
Describing the Sensor Location • 137, 138
Device Configuration • 167
Device Configuration Commands • 181
Device Management • 58
Diagnostic Commands • 292
Different CLI Modes and Prompts • 162, 163, 164, 181
Disabling the LDAP Authentication • 117
Displaying the Device Information • 59
Dominion PX Explorer Pane • 48
Downloading Diagnostic Information • 150
Downloading Key and Certificate Files • 112
Downloading SNMP MIB • 69, 156, 157, 158

E

Editing Firewall Rules • 100
Editing Ping Monitoring Settings • 132
Editing Role-Based Access Control Rules • 106
Editing the LDAP Server Settings • 117
Enabling Data Logging • 73
Enabling IPv4 or IPv6 • 185
Enabling LDAP and Local Authentication Services • 118
Enabling Login Limitations • 102
Enabling or Disabling a User Profile • 274
Enabling or Disabling Data Logging • 182
Enabling or Disabling EnergyWise • 286
Enabling or Disabling SNMP v1/v2c • 205
Enabling or Disabling SNMP v3 • 205
Enabling or Disabling SSH • 204
Enabling or Disabling Strong Passwords • 218
Enabling or Disabling Telnet • 203
Enabling Password Aging • 103
Enabling SNMP • 73, 155
Enabling Strong Passwords • 103
Enabling the Feature • 104
Enabling the Firewall • 96, 97
Enabling User Blocking • 101
EnergyWise Configuration Commands • 286
EnergyWise Settings • 178

Entering the Configuration Mode • 164, 181, 191, 272, 281
Entering the Diagnostic Mode • 164, 292
Environmental Sensor Configuration Commands • 228
Environmental Sensor Information • 40, 170
Environmental Sensor Threshold Information • 176
Environmental Sensors • 133
Example • 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 209, 210, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 225, 226, 227, 228, 229, 230, 231, 232, 234, 236, 237, 239, 240, 242, 243, 245, 246, 248, 250, 251, 252, 253, 254, 255, 256, 257, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 278, 280, 281, 283, 285, 286, 287, 288, 293, 294, 295
When Hysteresis is Useful • 87
When to Disable Hysteresis • 87
Example 1 - Basic Security Information • 180
Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 289
Example 2 - Combination of Upper Critical and Upper Warning Settings • 289
Example 2 - In-Depth Security Information • 180
Example 3 - Combination of SSID and PSK Parameters • 290
Examples • 179
Existing Roles • 178
Existing User Profiles • 177
Expanding the Tree • 49, 79, 80, 81, 82, 83, 84, 85, 134, 135, 136, 139, 142

F

Firewall Control • 208
Firmware Upgrade • 145, 150
Forcing a Password Change • 274
Forcing HTTPS Encryption • 66, 96, 107
Full Disaster Recovery • 153

G

Gathering the LDAP Information • 113

H

Help Command • 164
History Buffer Length • 179
How to Connect Differential Air Pressure Sensors • 31
How to Use the Calendar • 70, 71
HTTPS Access • 214

I

Identifying Environmental Sensors • 133, 134, 135
Idle Timeout • 217
Initial Network Configuration • 18, 44, 51, 60, 61, 304, 305
Installation and Configuration • 4
Installing a CA-Signed Certificate • 109
Installing Existing Key and Certificate Files • 111
Installing the USB-to-Serial Driver • 15
Introduction • 1
Introduction to the Web Interface • 47
IP Configuration • 165

L

LAN Interface Settings • 166
Layout • 159
LCD Display • 37, 39, 40
LCD Display Panel • 36
LDAP Configuration Illustration • 116, 306
Line Cord • 33
Listing TCP Connections • 148
Logging in to CLI • 161
Logging in to the Web Interface • 44
Logging out of CLI • 297
Login • 24, 44
Login Limitation • 215
Logout • 46
Logout Button • 53
Lowercase Character Requirement • 219

M

MAC Address • 14, 41
Mains Accuracy • 300
Mains Channel Configuration Commands • 228
Mains Channels • 34
Mains Information • 39, 169
Mains Pole Threshold Information • 175
Mains Threshold Information • 174
Managing Environmental Sensors • 133, 135
Managing Event Logging • 128
Managing Firewall Rules • 210

Managing Role-Based Access Control Rules • 224
Mapping Channels with Branch Circuits • 24
Maximum Ambient Operating Temperature • 5, 301
Maximum Password History • 222
Maximum Password Length • 219
Menus • 48
Minimum Password Length • 219
Modifying a Firewall Rule • 212
Modifying a Role • 91, 92, 94, 284
Modifying a Role-Based Access Control Rule • 225
Modifying a User Profile • 46, 91, 94, 271
Modifying a User's Personal Data • 273
Modifying an Action • 69, 127
Modifying an Event Rule • 126
Modifying the Firewall Control Parameters • 208
Modifying the IPv4 Settings • 63
Modifying the IPv6 Settings • 65
Modifying the Network Configuration • 60
Modifying the Network Interface Settings • 60
Modifying the Network Service Settings • 66, 161, 163
Modifying the Network Settings • 51, 62, 308
Modifying the Role-Based Access Control Parameters • 223
Modifying the SNMPv3 Settings • 275
Monitoring a Channel • 82
Monitoring All Channels • 81
Monitoring Server Accessibility • 131
Monitoring the Branch Circuit Channels • 81
Monitoring the Mains Channels • 80
More Information • 53
More Information about AD Configuration • 116
Multi-Command Syntax • 208, 215, 217, 218, 223, 271, 273, 275, 279, 289

N

Naming Branch Circuit Channels • 79
Naming the Branch Circuit Monitor • 49, 50, 51, 60, 72, 76, 77, 79, 80, 81, 83, 85, 134, 135, 136, 137, 139, 142
Naming the Mains Channels • 79
Network Configuration • 165
Network Diagnostics • 147
Network Service Settings • 167
Network Troubleshooting • 147, 292
Networking Configuration Commands • 184
Networking Mode • 166
Numeric Character Requirement • 220

O

Observing the Safety Guidelines and Instructions • 5
Operating the LCD Display • 38
Overriding the IPv4 DHCP-Assigned DNS Server • 196
Overriding the IPv6 DHCP-Assigned DNS Server • 199, 200
Overview • 1

P

Package Contents • 3, 4
Panel Components • 33
Password Aging • 216
Password Aging Interval • 216
Pinging a Host • 148
Power Measurement Accuracy • 300
Printing the Circuit Monitoring Worksheet • 5
Product Features • 2
Product Models • 1
Providing the EAP CA Certificate • 190

Q

Querying Available Parameters for a Command • 164, 296
Querying the DNS Servers • 293
Quitting the Configuration Mode • 181, 290
Quitting the Diagnostic Mode • 295

R

Raritan Current Transformers (Optional) • 8
Rebooting the Branch Circuit Monitor Device • 76
Reliability Data • 178
Reliability Error Log • 179
Reset Button • 42
Resetting the Branch Circuit Monitor • 291
Resetting to Factory Defaults • 42, 292, 304
Resizing a Dialog • 57, 59, 129, 149
Restarting the Device • 291
Retrieving Previous Commands • 296
Retrieving Software Packages Information • 153
RF Code Energy Monitoring Solution • 316
Role Configuration Commands • 281

Role of a DNS Server • 66, 308
Role-Bassed Access Control • 222

S

Safety Guidelines • iii, 5
Safety Instructions • iv, 5
Sample Branch Circuit-Level Event Rule • 126
Sample Device-Level Event Rule • 125
Sample Event Rules • 125
Sample Mains-Level Event Rule • 125
Saving a Branch Circuit Monitor Configuration • 144
Security Configuration Commands • 207
Security Settings • 177
Selecting IPv4 or IPv6 Addresses • 186
Selecting the Internet Protocol • 63, 65
Sensor Measurement Accuracy • 140
Sensor RJ-12 Port Pinouts • 302
Sensor Threshold Configuration Commands • 233
Serial RS-232 Port Pinouts • 301
Setting Data Logging • 73, 182
Setting Power Thresholds • 55, 83, 160
Setting the Authentication Method • 187
Setting the Branch Circuit Channel's Assertion Timeout • 241
Setting the Branch Circuit Channel's Deassertion Hysteresis • 239
Setting the Branch Circuit Channel's Lower Critical Threshold • 236
Setting the Branch Circuit Channel's Lower Warning Threshold • 238
Setting the Branch Circuit Channel's Upper Critical Threshold • 233
Setting the Branch Circuit Channel's Upper Warning Threshold • 235
Setting the Branch Circuit Pole's Assertion Timeout • 250
Setting the Branch Circuit Pole's Deassertion Hysteresis • 248
Setting the Branch Circuit Thresholds • 84, 85
Setting the BSSID • 192
Setting the Data Logging Measurements Per Entry • 182
Setting the Date and Time • 69
Setting the EAP Identity • 189
Setting the EAP Parameters • 188
Setting the EAP Password • 190
Setting the EnergyWise Configuration • 75
Setting the History Buffer Length • 289
Setting the Inner Authentication • 189
Setting the IPv4 Address • 194
Setting the IPv4 Configuration Mode • 193
Setting the IPv4 Gateway • 195
Setting the IPv4 Primary DNS Server • 195
Setting the IPv4 Secondary DNS Server • 196
Setting the IPv4 Subnet Mask • 194
Setting the IPv6 Address • 198
Setting the IPv6 Configuration Mode • 197
Setting the IPv6 Gateway • 198
Setting the IPv6 Primary DNS Server • 199
Setting the IPv6 Secondary DNS Server • 199
Setting the LAN Interface Parameters • 200
Setting the Lower Critical Threshold for a Branch Circuit Pole • 245
Setting the Lower Critical Threshold for an Inlet Pole • 260
Setting the Lower Warning Threshold for a Branch Circuit Pole • 247
Setting the Lower Warning Threshold for a Mains Pole • 261
Setting the Mains Channels' Assertion Timeout • 257
Setting the Mains Channels' Deassertion Hysteresis • 256
Setting the Mains Channels' Lower Critical Threshold • 254
Setting the Mains Channels' Lower Warning Threshold • 255
Setting the Mains Channels' Upper Critical Threshold • 252
Setting the Mains Channels' Upper Warning Threshold • 253
Setting the Mains Pole's Assertion Timeout • 263
Setting the Mains Pole's Deassertion Hysteresis • 262
Setting the Mains Thresholds • 83
Setting the Network Service Parameters • 201
Setting the Networking Mode • 184
Setting the Outer Authentication • 188
Setting the Polling Interval • 288
Setting the Preferred Host Name • 193
Setting the PSK • 188
Setting the Sensor's Assertion Timeout • 269
Setting the Sensor's Deassertion Hysteresis • 268
Setting the Sensor's Lower Critical Threshold • 266
Setting the Sensor's Lower Warning Threshold • 267
Setting the Sensor's Upper Critical Threshold • 265

Setting the Sensor's Upper Warning Threshold • 266
Setting the SNMP Configuration • 204
Setting the SNMP Read Community • 206
Setting the SNMP Write Community • 206
Setting the SSID • 187
Setting the sysContact Value • 206
Setting the sysLocation Value • 207
Setting the sysName Value • 207
Setting the Upper Critical Threshold for a Branch Circuit Pole • 242
Setting the Upper Critical Threshold for a Mains Pole • 257
Setting the Upper Warning Threshold for a Branch Circuit Pole • 243
Setting the Upper Warning Threshold for an Inlet Pole • 259
Setting the Wireless Parameters • 186
Setting the X Coordinate • 230
Setting the Y Coordinate • 231
Setting the Z Coordinate • 184, 231
Setting the Z Coordinate Format • 137
Setting the Z Coordinate Format for Environmental Sensors • 183, 232
Setting Up a Power Monitoring System • 7, 24
Setting Up an SSL Certificate • 95, 107
Setting Up LDAP Authentication • 66, 95, 112, 310
Setting Up Role-Based Access Control Rules • 104
Setting Up Roles • 45, 73, 88, 91, 93
Setting Up User Login Controls • 101
Setup Button • 51
Showing Information • 165
Showing the Network Connections • 293
Single Login Limitation • 215
SNMP Gets and Sets • 158
SNMP Sets and Thresholds • 160
Sorting Firewall Rules • 100
Sorting Role-Based Access Control Rules • 106
Sorting the LDAP Access Order • 116
Special Character Requirement • 221
Specifications • 298
Specifying the Device Altitude • 72, 183
Specifying the EnergyWise Domain • 287
Specifying the EnergyWise Secret • 287
Specifying the Sensor Type • 229
States of Managed Sensors • 140
Status Bar • 51
Step A. Determine User Accounts and Groups • 306
Step B. Configure User Groups on the AD Server • 307
Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device • 308
Step D. Configure Roles on the Branch Circuit Monitor • 311
Strong Passwords • 218
Supported Web Browsers • 43
Supported Wireless LAN Configuration • 17

T

Testing the LDAP Server Connection • 116
Testing the Network Connectivity • 294
The Branch Circuit Monitor MIB • 158
The Yellow- or Red-Highlighted Reading • 54, 58, 80, 81, 82, 139
Tracing the Network Route • 148
Tracing the Route • 295

U

Unblocking a User • 101, 291
Unmanaging Environmental Sensors • 136, 142
Unpacking the Product and Components • 4
Updating the Branch Circuit Monitor Firmware • 151
Uppercase Character Requirement • 220
User Blocking • 217
User Configuration Commands • 270
User Management • 88
Using SNMP • 152, 155
Using the CLI Command • 292, 305
Using the Command Line Interface • 66, 138, 161, 305
Using the Reset Button • 304
Using the Web Interface • 18, 43

V

Viewing Connected Users • 130
Viewing Firmware Update History • 152
Viewing Sensor Data • 139
Viewing the Communication Log • 52, 149
Viewing the Dashboard • 58
Viewing the Local Event Log • 129
Viewing the Webcam Images or Videos • 32, 147

W

Warning Icon • 53
What is Assertion Timeout? • 84, 85, 86, 88, 137, 241, 251, 257, 264, 270
What is Deassertion Hysteresis? • 83, 84, 85, 86, 128, 137, 240, 250, 256, 263, 269
Wired Network Settings • 60
Wireless Configuration • 166
Wireless Network Settings • 61
With HyperTerminal • 162, 291
With SSH or Telnet • 163

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com